Studie

STAATLICHE INITIATIVEN ZUR UNTERSTÜTZUNG DER IT-SICHERHEIT VORWIEGEND IN DER MITTELSTÄNDISCHEN WIRTSCHAFT IM INTERNATIONALEN VERGLEICH – INSBESONDERE IN EUROPA UND DEN USA

Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie

Projektbericht

Vorgelegt von:

Detecon International GmbH

Institut für Wirtschafts- und Politikforschung Schorn & Partner Wirtschaftswissenschaftler

Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.

30. Mai 2014



We make ICT strategies work

Inhaltsverzeichnis

Abbildungsverzeichnis II
Tabellenverzeichnis IV
Abkürzungsverzeichnis V
1 Die Ausgangssituation in Deutschland 9
1.1 Bedeutung und Stand der Informationssicherheit 9
1.2 Staatlicher Handlungsbedarf und Initiativen zur Informationssicherheit 13
2 Auftrag und Aufbau der Studie 15
2.1 Ziel und Gegenstand der Studie 15
2.2 Methodisches Vorgehen 16
3 Auswahl der untersuchten Länder 19
4 Vergleichsanalyse zu Stand der Informationssicherheit 34
4.1 Rahmen der Initiativen 35
4.2 Intentionen der untersuchten Initiativen 48
4.3 Ansätze und Mittel zur Verbesserung der Informationssicherheit 60
4.4 Wirkungen und Nachhaltigkeit der Initiativen 75
5 Informationssicherheit in ausgesuchten Ländern 78
5.1 Estland 78
5.2 Großbritannien 82
5.3 Niederlande 87
5.4 Österreich 91
5.5 Schweden 96
5.6 Spanien 99
5.7 USA 102
6 Handlungsoptionen 106
6.1 Phase 1: Bewusstsein schaffen 108
6.2 Phase 2: Lernen 108
6.3 Phase 3: Rat suchen und planen 109
6.4 Phase 4: Analysieren und testen 110
6.5 Phase 5: Vorfälle handhaben 110
Anhang A: Übersicht der untersuchten Initiativen 111
7 Literaturverzeichnis 143

Abbildungsverzeichnis

Abbildung 1: Vorgehen im Projekt (vereinfachte Darstellung) 17

Abbildung 2: Anteil der Unternehmen nach Beschäftigtengrößenklassen (2010) 19

Abbildung 3: Anteil der Beschäftigten nach Beschäftigtengrößenklassen (2010) 20

Abbildung 4: Anteile der Unternehmen (ab 10 Beschäftigten) mit hohem Technologieniveau bzw. wissensintensiven Dienstleistungen (2010) 21

Abbildung 5: Nutzung von Internetbanking und E-Commerce durch die Verbraucher (2012) 22

Abbildung 6: Anteil der Beschäftigten, die an das Internet angeschlossene Computer nutzen (2012) 23

Abbildung 7: Anteile der Unternehmen mit Sicherheitsproblemen im Berichtsjahr (2010) 24

Abbildung 8: Anteile der Unternehmen mit Bedenken bezüglich der Vertraulichkeit und Sicherheit der Daten in der Abwicklung elektronischer Verwaltungsvorgänge (2011) 25

Abbildung 9: Anteile der Unternehmen mit einer formell festgelegten Sicherheitspolitik einschließlich eines Konzeptes mit regelmäßiger Überprüfung (2010) 26

Abbildung 10: Anteile der Unternehmen, die Vorgänge zur Analyse von Sicherheitsproblemen protokollieren (2010) 27

Abbildung 11: Anteile der Unternehmen, die strenge Passwort- Authentifizierung oder Nutzeridentifizierung bzw. -authentifizierung via Hardware-Elemente verwenden (2010) 28

Abbildung 12: Anteile der Unternehmen, die externe Datensicherung verwenden (2010) 29

Abbildung 13: Anteil der Unternehmen, die fortschrittliche elektronische Signaturen in ihren Zulieferern- oder Kundenbeziehungen verwenden (2010) 30

Abbildung 14: Anteile der Unternehmen, die IKT-Aufgaben von externen Auftragnehmern erledigen lassen (2007) 31

Abbildung 15: Anteile der Unternehmen, die für Nicht-IKT-Beschäftigte IKT-Fortbildungsmaßnahmen durchführten (2012) 32

Abbildung 16: Anzahl betrachtete Initiativen aufgeteilt nach Ländern. 34

Abbildung 17: Politischer Kontext der Initiativen 36

Abbildung 18: Politischer Kontext der Initiativen 37

Abbildung 19:Die Akteure im Überblick 40

Abbildung 20: Die Akteure in den einzelnen Ländern 40

Abbildung 21: Die Adressaten im Überblick 44

Abbildung 22: Die Adressaten nach Ländern 45

Abbildung 23: Die Laufzeiten der Initiativen im Überblick 46

Abbildung 24: Die Laufzeiten der Initiativen nach Ländern 47

Abbildung 25: Ziele im Hinblick auf die Informationssicherheit im Überblick 49

Abbildung 26: Ziele im Hinblick auf die Informationssicherheit 50

Abbildung 27: Einfluss der Initiativen auf die Dimensionen einer Kultur der Informationssicherheit im Überblick...53

Abbildung 28: Einfluss der Initiativen auf die Dimensionen einer Kultur der Informationssicherheit nach Ländern..54

Abbildung 29: Die von den Initiativen aufgegriffenen Gründe für mangelnde Informationssicherheit im Überblick...55

Abbildung 30: Die von den Initiativen aufgegriffenen Gründe für mangelnde Informationssicherheit nach Ländern..55

Abbildung 31: Zuordnung der Initiativen zu den Maßnahmenkatalogen des BSI im Überblick 61

Abbildung 32: Zuordnung der Initiativen zu den Maßnahmenkatalogen des BSI nach Ländern 61

Abbildung 33: Genutzte Ressourcen im Überblick 63

Abbildung 34: Genutzte Ressourcen nach Ländern 63

Abbildung 35: Die genutzten Instrumente im Überblick..65

Abbildung 36: Die genutzten Instrumente nach Ländern 66

Abbildung 37: Instrumente nach den durch die Initiative aufgegriffenen Gründen mangelnder Informationssicherheit...67

Abbildung 38: Die Schnittstellen der Initiativen im Überblick 73

Abbildung 39: Die Schnittstellen der Initiativen nach Ländern 74

Abbildung 40: Zyklus zur Schaffung von Informationssicherheit..106

Abbildung 41: Die Initiativen nach Phasen im Überblick 107

Abbildung 42: Die Initiativen nach Phasen und Ländern..107

Tabellenverzeichnis

Tabelle 1: Definition kleiner und mittelständischer Unternehmen laut Europäische Kommission 16

Abkürzungsverzeichnis

Allgemeine Abkürzungen

BYOD	Bring-Your-Own-Device
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and Related Technology
DNS	Domain Name System
ENISA	European Network and Information Security Agency
EU	Europäische Union
IKT	Informations- und Kommunikationstechnik
ISM	Informationssicherheits-Management
ISMS	Informationssicherheits-Managementsystem
ISO	Internationale Organisation für Normung
KMU	Kleine und mittlere Unternehmen
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
SME	Small and medium-sized enterprises
VwVfG	Verwaltungsverfahrensgesetz

Landesspezifische Institutionen und Initiativen

Abkürzung	Originalbezeichnung (Offizielle englische Bezeichnung)	Land
APWG	Anti-Phishing Working Group	USA
A-SIT	Zentrum für sichere Informationstechnologie – Austria	Österreich
BCRC	Business Crime Reduction Centre	Großbritannien
BIS	Department for Business, Innovation and Skills	Großbritannien
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien	Deutschland
BMI	Bundesministerium des Innern	Deutschland
BMWi	Bundeministerium für Wirtschaft und Energie	Deutschland
BSI	Bundesamt für Sicherheit in der Informationstechnologie	Deutschland
CCI	Centro de Ciberseguridad Industrial (Industrial Cybersecurity Center)	Spanien
CESG	Communications-Electronics Security Group	Großbritannien

Abkürzung	**Originalbezeichnung** **(Offizielle englische Bezeichnung)**	**Land**
CPNI	Platform voor Cybersecurity (Centre for Protection of the National Infrastructure)	Niederlande
CSA-ES	Cloud Security Alliance España	Spanien
CSAN	Cyber Security Assessment Netherlands	Niederlande
CNCCS	Consejo Nacional Consultor sobre Cyber Seguridad	Spanien
CREST	Council of Registered Ethical Security Testers	Großbritannien
DHS	Department of Homeland Security	USA
DsiN e.V	Deutschland sicher im Netz e.V.	Deutschland
FBI	Federal Bureau of Investigation	USA
FCC	Federal Communications Commission	USA
GCHQ	Government Communications Headquarters	Großbritannien
INTECO	Instituto Nacional de Tecnologías de la Comunicación (National Institute of Communication Technologies)	Spanien
ISB	Informatikstrategieorgan des Bundes	Schweiz
ISIS	IT och Säkerhet i Inre Skandinavien (IT Security in Scandinavia)	Schweden
ISMS	Asociación Española para el Fomento de la Seguridad de la Información (Spanish Association for the Development of Information Security)	Spanien
JVO	Järelevalve Osakond (Supervision Department)	Estland
KIIK	Kriitilise Info Infrastruktuuri Kaitse Osakond (Critical Information Infrastructure Department)	Estland
KTH	Kungliga Tekniska högskolan (Royal Institute of Technology)	Schweden
KSÖ	Kuratorium Sicheres Österreich	Österreich
MKB	Koninklijke Vereniging MKB-Nederland (Royal Association MKB-Nederland)	Niederlande
MSB	Myndigheten för samhällsskydd och beredskap (Swedish Civil Contingencies Agency)	Schweden
NCSA	National Cyber Security Alliance	USA
NCSC	National Cyber Security Centrum (National Cyber Security Centre)	Niederlande

Abkürzung	Originalbezeichnung (Offizielle englische Bezeichnung)	Land
NISÖ	Nationell informationssäkerhetsövning	Schweden
	(National Cyber Security Excercise)	
NIST	National Institute of Standards and Technology	USA
NCSS	National Cyber Security Strategy	Niederlande
NSA	National Security Agency	USA
NSS	National Security Strategy	Großbritannien
OCSIA	Office of Cyber Security & Information Assurance	Großbritannien
ÖSCS	Österreichische Strategie für Cyber Sicherheit	Österreich
PTS	Post- och telestyrelsen	Schweden
	(Post and Telecom Authority)	
RIA	Riigi Infosüsteemi Amet	Estland
	(Estonian Information System Authority)	
RISO	Riigi Infosüsteemid	Estland
	(Department of State Information Systems)	
RVO	Rijksdienst voor Ondernemend Nederland	Niederlande
	(Netherlands Enteroprise Agency)	
SBA	US Small Business Administration	USA
SBIR	Small Business Innovation Research	Niederlande
SIHA	Österreichisches Informationssicherheitshandbuch	Österreich
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	Niederlande
	(Netherlands Organisation for Applied Scientific Research)	
TSB	Technology Strategy Board	Großbritannien
UBIT	Fachverbands Unternehmensberatung, Buchhaltung und Informationstechnologie der WKO	Österreich
VNO-NCW	Verbond van Nederlandse Ondernemingen (VNO) en het Nederlands Christelijk Werkgeversverbond	Niederlande
	(Confederation of Dutch Industry and Employers)	
WKO	Wirtschaftskammer Österreich	Österreich

Im nachfolgenden Text wird für ein besseres Leseverständnis und einen flüssigeren Sprachstil die männliche Grammatikform generisch verwendet.

Die Autoren danken den zahlreichen Behördenvertretern und IT-Sicherheitsexperten, die an den Interviews teilgenommen haben und damit einen wertvollen Beitrag zur Identifikation und Dokumentation relevanter Initiativen in den betrachteten Ländern geleistet haben. Darüber hinaus danken wir den Teilnehmern des Experten-Workshops, der im Rahmen der Erarbeitung der Studie im April in Berlin stattgefunden hat.

1 Die Ausgangssituation in Deutschland

1.1 Bedeutung und Stand der Informationssicherheit

Informationstechnologie (IT) hat im deutschen Mittelstand eine sehr hohe einzelwirtschaftliche Bedeutung. Nahezu alle (99,7 Prozent) kleinen und mittleren Unternehmen (KMU) setzen IT-Systeme zur Unterstützung ihrer Geschäftsprozesse ein und eine große Mehrheit (80 Prozent) der Mittelständler nutzen das Internet zur Bereitstellung von Informationen und Dienstleistungen (Büllingen und Hillebrand 2012). Aufgrund der steigendenden Komplexität der IT-Landschaft, gehen auch KMU zunehmend dazu über, IT-Dienste extern einzukaufen. So ließen nach einer Erhebung von Eurostat 2007 61% der Unternehmen mit 10 bis 49 Beschäftigten und 82% derjenigen mit 50 bis 249 Beschäftigten Aufgaben der IKT von externen Auftragnehmern erledigen. Nach Büllingen und Hillebrand (2012) nutzen immerhin noch mehr als 32 Prozent Outsourcing und 10 Prozent der KMU setzen auf flexible und innovative Lösungen, wie z.B. Cloud Computing. Zwar hat nach den Ergebnissen des Cloud-Monitors 2014 die NSA-Affäre dem „Wachstum einen Dämpfer versetzt“[1], dennoch ist die Zahl der Nutzer von Cloud Computing in den vergangenen Jahren kontinuierlich gestiegen. In 2013 hatten bereits 15% der Unternehmen mit 20 bis 99 Beschäftigen eine Public Cloud und 33% dieser Gruppe eine Private Cloud im Einsatz.

Die hohe Verbreitung und damit auch Abhängigkeit von der IT birgt Risiken für den Mittelstand. Unternehmen sehen sich im digitalen Zeitalter einer Reihe neuartiger Gefahren gegenüber. Während Unternehmen jedoch in der realen Welt Räume abschließen, einen Brandschutz einbauen oder Transporte gegen Raub versichern, unterlassen sie in der virtuellen Welt oftmals vergleichbare Sicherheitsmaßnahmen. Dabei handelt es sich in Anbetracht der vielfältigen Varianten, einen Schaden erleiden zu können, nicht nur um ein kleines oder punktuelles Risiko. Für ein Unternehmen können Schäden durch technisches Versagen, unabsichtliches Fehlverhalten von Mitarbeitern oder durch vorsätzliches Handeln entstehen. Gerade Letzteres hat infolge der zunehmenden Vernetzung (Botnetze, DNS- und Routing-Manipulationen, Smart Grid), technischen Schnittstellen (Mobilkommunikation, E-Mail und andere Anwendungssoftware) und verfügbaren Werkzeuge (Drive-By-Exploits, Spam, Trojaner, Schadsoftware und Phishing) an Bedeutung gewonnen (BSI 2011a).

Je nach Studie und Gliederung der Schadensursachen variiert die jeweilige relative Bedeutung technischer und menschlicher – absichtlicher oder unabsichtlicher – Störungen. Die mit Abstand häufigste Ursache für ein IT-Sicherheitsproblem im deutschen Mittelstand ist nach Büllingen und Hillebrand (2012) der Ausfall der IT-Systeme mit einem Anteil von 79 Prozent der befragten Unternehmen. Ebenfalls ohne kriminellen Hintergrund sind die Schäden aus unabsichtlichen Datenverlusten, die von 41 Prozent der Unternehmen genannt wurden. Dazwischen liegen Virenangriffe mit 51 Prozent und Spam mit 74 Prozent. Ein wenig anders sieht die Gewichtung nach einer Befragung durch das Ponemon Institute (2013) aus. Hier liegt die Hauptursache für einen Datenverlust zu 48 Prozent in Schadsoftware und kriminellen Attacken, zu 35 Prozent im menschlichen Faktor und zu 16 Prozent in einer Systemstörung.

Die Vorfälle betreffen nicht nur spezielle oder große Unternehmen oder solche spezieller Branchen, sondern ebenso ein breites Spektrum von KMU. Zwar sind größere Unternehmen

[1] Vgl. hierzu die gemeinsame Pressekonferenz von BITKOM und KPMG (Kempf und Wallraf 2014).

tatsächlich häufiger mit Sicherheitsvorfällen konfrontiert, kleinere Unternehmen stehen dem jedoch nur geringfügig nach. So haben in Deutschland lediglich 7 Prozent der Unternehmen mit bis zu 49 Mitarbeitern bislang keine Erfahrungen mit einem IT-Sicherheitsvorfall gemacht (Büllingen und Hillebrand 2012).

Die Häufigkeit, mit der auch KMU von IT-Sicherheitsvorfällen betroffen sind, weist bereits auf die Bedeutung des Themas für die mittelständische Wirtschaft hin. Allerdings ist nicht jeder Vorfall derart bedeutsam, dass sich ein Unternehmen zu zeitlichen und finanziellen Investitionen in die IT-Sicherheit veranlasst sähe. Die veröffentlichten Studien zeigen je nach Quelle und Definition unterschiedliche Schadenshöhen. Büllingen und Hillebrand (2012) ermitteln für 19 Prozent der deutschen Unternehmen bis 500 Mitarbeitern eine Beeinträchtigung des Geschäfts von mindestens einem Tag, wobei Unternehmen mit mindestens 50 Mitarbeitern Probleme im Durchschnitt etwas schneller lösen können. Geschonneck und Fritzsche (2013) ermitteln für Deutschland, beschränkt auf Cyberkriminalität und über alle Unternehmensgrößenklassen hinweg, einen durchschnittlichen Schadensbetrag von rund 100.000 Euro für einen einzelnen Deliktsfall einschließlich der Folgekosten. Duscha et al. (2011) bestimmen Kosten von mindestens 20.000 Euro, die für fast jedes zehnte befragte KMU in Folge einer Cyberattacke entstehen. Bei knapp 60 Prozent der Unternehmen lag der Schaden bei weniger als 1.000 Euro. Büllingen und Hillebrand (2012) weisen darauf hin, dass die vorstehende Befragung nicht als repräsentativ erachtet werden kann. In einer durch die Initiative „IT-Sicherheit in der Wirtschaft“ geförderten Veröffentlichung reicht die Schadenshöhe in den dort geschilderten Fallbeispielen deutscher Mittelständler von 1.000 bis zu 500.000 Euro (Bundesverband mittelständische Wirtschaft 2013). Der Mehrländervergleich für 2012 durch das Ponemon Institute (2013) ermittelt für Deutschland – über alle Unternehmensgrößen hinweg – durchschnittliche Kosten aufgrund verlorener oder gestohlener Daten in Höhe von 4,8 Millionen US-Dollar (umgerechnet ca. 3,5 Millionen Euro).

Die Relevanz des Themas wird nochmals deutlicher, wenn man den Kosten, die für ein Einzelunternehmen infolge eines Sicherheitsvorfalls entstehen, auch den gesamtwirtschaftlichen Schaden hinzurechnet. Dieser entsteht insbesondere dadurch, dass Unternehmen aufgrund von Sicherheitsbedenken bewusst Transaktionen im Internet unterlassen. So verzichten 47 Prozent der vom BITKOM 2012 befragten Unternehmen ganz oder teilweise auf die Nutzung von Transaktionen, die per Internet durchgeführt werden können[2]. Somit bleiben viele Potenziale des Internets ungenutzt.

Die Bedeutung der IT-Sicherheit spiegelt sich schließlich auch in den Ausgaben der Unternehmen wider. Größere Mittelständler gaben an, im Durchschnitt 19.800 Euro in Maßnahmen zur Erhöhung der IT-Sicherheit investieren zu wollen (Büllingen und Hillebrand 2012). Für Kleinunternehmen ergab sich eine geplante Investitionssumme von 3.100 Euro. Dementsprechend wichtig ist mittlerweile der Dienstleistungs- und Lösungsmarkt für IT-Sicherheit. In einer aktuellen Untersuchung im Auftrag des BMWi ermittelten Schubert und Rhiel (2013) ein Marktvolumen von 6,6 Milliarden Euro für Deutschland im Jahr 2012.

Angesichts der Bedeutung der Informationssicherheit ist anzunehmen, dass deutsche Mittelständler einen hohen Sicherheitsstandard besitzen. In der Realität zeigt sich allerdings ein anderes Bild. So geht in den zuvor erwähnten durchschnittlichen Investitionsbetrag von Kleinunternehmen auch ein Anteil von 33 Prozent der Unternehmen ein, die keinerlei Investitionen in ihre IT-Sicherheit planen. Ebenfalls einer differenzierten Betrachtung

[2] Vgl. hierzu die gemeinsame Pressekonferenz von BITKOM und BKA (Kempf 2012).

bedürfen die im Einzelnen getroffenen Sicherheitsvorkehrungen. Viele Unternehmen verfügen über Virenschutz und Firewall, weitergehende technische Maßnahmen – z.B. die Verschlüsselung von Daten oder die Sicherung von Datenservern – werden jedoch nur von einer Minderheit vorgenommen (Büllingen und Hillebrand 2012). Deutliche Defizite finden sich auch bei der Betrachtung der organisatorischen Vorkehrungen. Einfache Maßnahmen wie wirkungsvolle Schulungen zur IT-Sicherheit oder existenzsichernde Notfallpläne sind selbst in größeren mittelständischen Unternehmen keine Selbstverständlichkeit. Diese Ergebnisse werden durch die Erkenntnisse einer Untersuchung durch das BSI (2011b) bestätigt, in deren Rahmen der Reifegrad der IT-Sicherheit in Anlehnung an den IT-Grundschutz vor Ort bei mittelständischen Unternehmen im Detail analysiert wurde. Im Fazit der IT-Sicherheitsexperten zeigt sich, dass eine deutliche Mehrheit der KMU Maßnahmen zur Sicherheit der eigenen Netze ergriffen hat. Entsprechende Schritte im Hinblick auf die im Unternehmen genutzten Anwendungen oder das Vorhandensein eines Notfallmanagements wurden hingegen nur in rund der Hälfte der teilnehmenden Unternehmen eingeführt. Brandl und Scharioth (2013) stellen durch die Auswertung von über 1.500 IT-Sicherheitschecks einen Trend zu erhöhten Sicherheitsmaßnahmen über die letzten Jahre fest. Die im Vergleich zu anderen Studien höheren Anteile sicherheitsbewusster Unternehmen sollten jedoch nicht überinterpretiert werden, da die Teilnahme an einem Sicherheitscheck bereits auf eine fortgeschrittene Kenntnis des Themas IT-Sicherheit schließen lässt. Weiterhin ist zu beachten, dass trotz eines erhöhten Sicherheitsbewusstseins bei den befragten Unternehmen trotzdem weitere Optimierungspotentiale (z.B. beim E-Mail-Schutz) zu erschließen sind.

Im Vergleich zu den anderen Mitgliedsstaaten der Europäischen Union liegt Deutschland in Bezug auf die Adaption technischer und organisatorischer Maßnahmen bei IKT-Nutzung und elektronischem Handel in Unternehmen im Mittelfeld.[3] 31% der deutschen Unternehmen haben eine IKT-Sicherheitspolitik formal definiert, wobei der Anteil in der Klasse der Kleinunternehmen nur bei 22% liegt. Ansätze zur Bewusstseinsbildung der Beschäftigten mit Bezug auf IT-Sicherheit verfolgt die Hälfte der befragten deutschen Unternehmen. Der Häufigkeit des Einsatzes technischer Methoden zur Authentifizierung und Datensicherung variiert je nach Instrument zwischen 15% (hardwarebasierte Authentifizierung) und 55% (externe Datensicherung).

Im Kontrast zu dem offensichtlichen Optimierungspotential steht – zumindest in Teilen – die Selbsteinschätzung deutscher Mittelständler. Während nahezu alle Unternehmen bereits Sicherheitsvorfälle zu beklagen hatten, betrachten nur 35 Prozent der von Büllingen und Hillebrand (2012) befragten Unternehmen das Niveau ihrer IT-Sicherheit als verbesserungsbedürftig. Der Grund für diese scheinbare Diskrepanz zwischen dem objektiv Wünschenswertem und dem tatsächlichem Stand liegt aber nicht einfach nur in der Fahrlässigkeit der Verantwortlichen. Wie Eichfelder und Schorn (2012) zeigen, entscheiden Unternehmen – im Rahmen der verfügbaren Informationen und vorhandenen Informationsverarbeitungskapazitäten – in Bezug auf die gewählten Bearbeitungsstrategien durchaus rational. Um die Informationssicherheit in mittelständischen Unternehmen nachhaltig zu verbessern, gilt es also die Gründe für die Ratio der Entscheider sowie für eine mögliche Verzerrung derselben zu verstehen.

Auf den ersten Blick erscheint es in Anbetracht der festgestellten Defizite in der Tat verwunderlich, dass die IT-Sicherheit für rund zwei Drittel der deutschen Mittelständler eine

[3] Vgl. hierzu im Detail Giannakouris und Smihily (2011) sowie auch Kapitel 3.

hohe oder gar sehr hohe Bedeutung besitzt[4]. Noch deutlicher fällt die Einschätzung zum eigenen Schutzbedarf aus. Hier beurteilen – je nach Art des Sicherheitsvorfalls – zwischen 76% und 82% der Unternehmen den Bedarf als mindestens hoch (Büllingen und Hillebrand 2012). Selbst wenn Unternehmer die Gefahren aus der IKT nicht immer realistisch einzuschätzen vermögen, ist ein Problembewusstsein dennoch durchaus vorhanden. Allerdings müssen Unternehmen ihre Entscheidungen abwägen, weshalb nicht jede die Sicherheit erhöhende Maßnahme rational vertretbar ist. Das Kalkül deutscher Mittelständler zeigt sich bei Büllingen und Hillebrand (2012) und Teuteberg (2010) in den Gründen für das Ausbleiben von Verbesserungen der IT-Sicherheit respektive der Umsetzung eines IT-Risikomanagements. Die dort am häufigsten genannten Gründe sind finanzielle und zeitliche Aufwände. In diesem Punkt zeigt sich der Effekt steigender Skalenerträge. Da der Aufwand zur Implementierung von Maßnahmen zur IT-Sicherheit oftmals mehr oder weniger unabhängig von der Zahl der IT-Arbeitsplätze ist, stellen die Kosten für Mittelständler eine wesentlich höhere Barriere dar als für Großunternehmen. Lizenzen werden zwar in der Regel nach der Anzahl genutzter Arbeitsplatz-Systeme berechnet, der grundsätzliche Administrationsaufwand zur Einführung und Pflege eines Systems ist jedoch relativ unabhängig von der Anzahl Nutzer zu erbringen.

Im Zusammenhang mit den durch die IT-Sicherheit verbundenen Aufwänden sehen sich Unternehmen neben den Kosten zur Einführung, auch mit dem von Albrechtsen (2007) festgestellten Konflikt zwischen Funktionalität und Sicherheit konfrontiert. Die Pflege von Dokumentationen, die Eingabe mehrerer komplexer Passwörter oder die Verschlüsselung von E-Mails im Austausch mit externen Mitarbeitern kann den Geschäftsbetrieb in der Wahrnehmung der Geschäftsführung und der Mitarbeiter unverhältnismäßig beeinträchtigen, so dass IT-Sicherheit mehr als Bürokratismus denn als notwendige Risikovorsorge empfunden wird. Zusammenfassend kommt Albrechtsen (2007) auf Basis von Interviews zu dem Ergebnis, dass die befragten Unternehmen die Benutzerfreundlichkeit und Effizienz gegenüber der Sicherheit priorisieren und so auch mit ihrer derzeitigen Situation zufrieden sind. Ein entsprechender empirischer Befund für Deutschland findet sich bei Duscha et al. (2011), die zu dem Schluss kommen, dass deutsche KMU eine Verbesserung des IT-Sicherheitsstandards zugunsten erhöhter Praktikabilität aufgeben.

Ein weiterer Grund für mangelhafte IT-Sicherheit findet sich in der Inhaberzentrierung von KMU (Ghobakhloo et al. 2011). Inhaber sind häufig im Tagesgeschäft eingebunden oder Ihnen fehlt die Nähe zur IT. Der ebenfalls häufig genannte Grund, dass KMU nicht über eine eigene IT-Abteilung verfügen, genügt allein nicht aus. Inhaber könnten das notwendige Wissen bei externen Dienstleistern (z.B. über Outsourcing) einkaufen. Diese Option wird jedoch aufgrund der Überschätzung der eigenen Effizienz oder von Misstrauen nicht immer genutzt, wie Ghobakhloo et al. (2011) allgemein und Eichfelder und Schorn (2012) speziell für Deutschland feststellen.

Darüber hinaus wird das fehlende Angebot an passenden Lösungen und Schulungen zu IT-Sicherheit in der Literatur als Ursache für nicht ausreichenden IT-Schutz identifiziert. Die Unübersichtlichkeit der Angebote wird von 52 Prozent, die mangelnde Verfügbarkeit geeigneter Lösungen von immerhin noch 17 Prozent der deutschen Mittelständler beklagt (Büllingen und Hillebrand 2012). Ferner scheint die fehlende Zielgruppenorientierung ein im

[4] Vgl. zur Bedeutung der IT-Sicherheit in deutschen KMU u.a. Büllingen und Hillebrand (2012) sowie Duscha et al. (2011).

Hinblick auf die Adaption von IT-Lösungen bestehendes Problem zu sein, wie der Literaturüberblick von Ghobakhloo et al. (2011) belegt.

1.2 Staatlicher Handlungsbedarf und Initiativen zur Informationssicherheit

In Zusammenfassung lässt sich festhalten, dass die Gründe für die Defizite in der Informationssicherheit deutscher Mittelständler zu einem wesentlichen Teil größenspezifisch sind. Insofern liegt es nahe, dass der Staat solche größenbedingten Nachteile im Rahmen der Mittelstandspolitik durch gezielte Initiativen zu mindern versucht. In Bezug auf die digitale Sicherheit fügt sich darüber hinaus noch ein Argument aus der analogen Welt an: Zwar sind Unternehmen grundsätzlich selbst für ihre Sicherheit verantwortlich, dennoch gehört die Prävention zum Schutz vor Einbruch oder anderen Delikten zu den Aufgaben der Sicherheitsbehörden. Insbesondere technologisch hochgerüstete Angreifer besitzen „Waffen“, die ihnen ein eindringen in die IT-Umgebung des Unternehmens ermöglichen und denen die meisten Unternehmen nicht gewachsen sind. Deshalb ist ein staatlicher Eingriff nicht nur ratsam erscheint, sondern geradezu geboten ist. Diesem Gebot hat die Bundesregierung mit der 2011 vorgestellten Cyber-Sicherheitsstrategie für Deutschland (Bundesministerium des Innern 2011) Rechnung getragen. Die beschlossenen Maßnahmen dienen im Kern dem Schutz kritischer Informationsinfrastrukturen. Dabei fokussieren die Bemühungen aber nicht nur auf die Unternehmen, die eine solche Infrastruktur bereitstellen, sondern ebenso auf deren Nutzer dieser Infrastruktur und der darauf aufbauenden IT-Systeme. Um den besonderen Bedürfnissen kleiner und mittlerer Unternehmen im Hinblick auf den sicheren Einsatz von IT-Systemen gerecht zu werden, wurde daher im Zuge der Umsetzung der Cyber-Sicherheitsstrategie unter anderem die Task Force „IT-Sicherheit in der Wirtschaft“ beim BMWi eingerichtet.

Die Task Force, die zwischenzeitlich mit der Reorganisation des Ministeriums nach der Bundestagswahl 2013 als dauerhafte Einrichtung in „Initiative ‘IT-Sicherheit in der Wirtschaft‘“ umbenannt wurde, hat seit ihrer Gründung bereits eine Vielzahl von einzelnen Initiativen auf den Weg gebracht. So werden bzw. wurden von den 21 deutschen Initiativen, die in diese Studie eingegangen sind, allein elf durch die Task Force gefördert[5].

Dabei wird ein breites Spektrum von Ansätzen, die von Maßnahmen zur Steigerung der Aufmerksamkeit bis zur Behandlung von Vorfällen reichen, genutzt. Im Einzelnen gehören dazu Kampagnen zur Bewusstseinsbildung, wie z.B. die Initiative *[m]it Sicherheit* des Bundesverbands mittelständische Wirtschaft (BVWM), der erste deutsche IT-Sicherheitspreis für KMU oder die Posterkampagne des BMWi, ebenso wie die Lernangebote der BITKOM-Akademie zu Online-Seminaren speziell für KMU oder des TeleTrust e.V. zu Workshops für Hotelbetriebe. Eine besondere Form von Schulungen bietet der Deutschland sicher im Netz e.V. (DsiN). In Workshops werden Rechtsanwälte, Wirtschaftsprüfer, Steuer- und Unternehmensberater mit den Grundlagen der IT-Sicherheit vertraut gemacht, um als Multiplikatoren ihren Klienten das Thema nahe zu bringen. Einen ähnlichen Ansatz verfolgt eine Initiative unter Beteiligung der Handwerkskammern, indem deren Betriebsberater als IT-Sicherheitsbotschafter geschult werden.

Darüber hinaus wurden im Rahmen der Task Force Initiativen initiiert, die KMU konkrete Hilfestellungen geben. Die *Initiative-S* des Verbands der deutschen Internetwirtschaft (eco)

[5] Eine Übersicht zu allen in dieser Studie untersuchten Initiativen findet sich im Anhang.

prüft Websites von KMU und unterstützt diese bei der Bereinigung von Schadsoftware, die *Information-Sicherheits-Analyse* (ISA+) soll in Zukunft KMU eine angepasste Zertifizierung erlauben und das Projekt *PROF[IT]ABEL* eine bessere Einschätzung der Kosten-Nutzen-Relation von Investitionen in IT-Sicherheit erlauben.

Das BMWi förderte und fördert auch außerhalb der Task Force Projekte zur IT-Sicherheit in KMU. So beteiligte es sich bereits 2006 bis 2009 am Aufbau des *Kompetenzzentrums für IT-Sicherheit und qualifizierte digitale Signatur* der Handwerkskammer Rheinhessen (komzet@hwk) und finanzierte 2007 bis 2011 die Entwicklung innovativer Sicherheitstechnologien im Rahmen des Technologieprogramms *Sichere Anwendung der mobilen Informationstechnik (IT) zur Wertschöpfungssteigerung in Mittelstand und Verwaltung* (SimoBIT). Aktuell unterstützt das Ministerium mit dem Programm *Trusted Cloud* als Bestandteil der IKT-Strategie „Deutschland Digital 2015“ und der „Hightech-Strategie“ der Bundesregierung die Entwicklung und Einführung von Cloud Computing-Lösungen, damit gerade mittelständische Unternehmen frühzeitig von den Chancen dieser Technologien profitieren können.

Zu den Initiativen ohne finanzielle Förderung des BMWi gehören das *Bürger-CERT* des Bundesamtes für Sicherheit in der Informationstechnik, das Bürgern sowie KMU zur Information über aktuelle Bedrohungen zur Verfügung steht und der *DsiN-Sicherheitscheck*, der Unternehmen eine erste Einschätzung der eigenen IT-Sicherheit bietet. Außerdem sind die Initiativen auf Landesebene zu erwähnen. Während Nordrhein-Westfalen mit der Initiative *nrw.units* die Vernetzung von IT-Dienstleistern und KMU fördert, führt das bayerische IT-Sicherheitscluster – zum Teil mit Unterstützung des BMWi – verschiedene Projekte durch, die Unternehmen allgemein und auch kleinen im speziellen Sicherheitslösungen anbieten.

Zusammenfassend ist festzustellen, dass der Staat seiner Aufgabe, Unternehmen durch Prävention zu schützen, durchaus nachkommt. Inwieweit das Angebot jedoch geeignet ist, die Informationssicherheit in KMU tatsächlich signifikant zu verbessern, lässt sich angesichts der noch beschränkten Erfahrungen mit der Wirkung dieser Initiativen derzeit nicht abschließend und belegbar beurteilen. Zwar gab es auch in der Vergangenheit bereits Bemühungen, KMU bei der IT-Sicherheit zu unterstützen, das Gros der Initiativen hat seinen Ursprung aber in 2011 oder später. An dieser Stelle setzt das vom BMWi in Auftrag gegebene Forschungsprojekt an, indem es durch einen Vergleich mit den Initiativen anderer Länder deren Ziele und Inhalte erfasst, um Schwerpunkte und Trends zu identifizieren und so zur Entwicklung zukünftiger Maßnahmen des BMWi in einem möglichst frühen Stadium nutzbar zu machen.

Der vorliegende Bericht stellt in Kapitel 2 die Methode und Vorgehensweise der Untersuchung vor und gibt in Kapitel 3 einen Überblick zu den verfügbaren Zahlen des statistischen Amtes der Europäischen Union (Eurostat) im Zusammenhang mit der IT-Sicherheit in KMU. Unter Berücksichtigung dieser Zahlen sowie qualitativer Überlegungen wurden die Länder ausgewählt, die im Weiteren bei der Vergleichsanalyse berücksichtigt wurden, deren Ergebnisse in Kapitel 4 dargestellt werden. Kapitel 5 erläutert dann die Ansätze und Rahmenbedingungen der einzelnen Länder im Detail, bevor schließlich Kapitel 6 die aus der Vergleichsanalyse und den Länderberichten resultierenden Handlungsoptionen erläutert.

2 Auftrag und Aufbau der Studie

2.1 Ziel und Gegenstand der Studie

Das dem Projekt übergeordnete Ziel besteht in der Verbesserung der Informationssicherheit in deutschen KMU. IT-Sicherheit ist allerdings kein Selbstzweck, sondern bietet einen betriebswirtschaftlichen Nutzen für Unternehmen. Durch das Sicherstellen eines reibungslosen Betriebs der notwendigen Geschäftsprozesse sowie der Verfügbarkeit aller relevanten Daten und Informationen sind Unternehmen in der Lage, effizienter als ihre Wettbewerber zu agieren. Darüber hinaus stellt eine sichere digitale Infrastruktur eines Unternehmens ein Alleinstellungsmerkmal dar, welches speziell im datenschutzsensiblen Wirtschaftsraum Deutschlands einen weiteren Wettbewerbsvorteil schafft. Weiterhin ist Informationssicherheit zur Sicherung der deutschen Wettbewerbsfähigkeit und geostrategischer Interessen der deutschen Wirtschaft im Kontext der globalen Cyberkriminalität von elementarer Bedeutung. Speziell der Vorfall in Estland im April 2007 hat den europäischen Nachbarn verdeutlicht, welche gravierenden Schäden durch gezielte Cyberattacken verursacht werden können. Solche Attacken auf staatliche Institutionen wie auch auf wirtschaftliche Akteure muss Deutschland als Staat bestmöglich zu unterbinden und verhindern wissen. Als Prämisse bei der Ausarbeitung des Projektkonzepts ist daher zu beachten, dass die einzelnen Schritte geeignet sind, einen Mehrwert stiftenden Nutzen durch eine Verbesserung der Informationssicherheit zu realisieren.

Im Ergebnis verfolgt das Projekt das konkrete Ziel, für das BMWi zukünftige Initiativen und Maßnahmen zu identifizieren, die geeignet sind, die Informationssicherheit in KMU in Deutschland zu fördern. Zu diesem Zweck ist es die Aufgabe der Auftragnehmer, Schwerpunkte und Trends durch den Vergleich entsprechender Initiativen der USA und der weiteren ausgewählten europäischen Länder zu ermitteln. Es gilt, aus dem Vergleich der erfassten Initiativen Impulse für mögliche Maßnahmen für KMU in Deutschland abzuleiten und dem Auftraggeber Möglichkeiten aufzuzeigen, diese zu initiieren. Grundlage des Vergleichs sind gemäß der Auftragsbeschreibung die Unterstützungsmaßnahmen des BMWi. Der Vergleich soll die Erfassung der Ziele und Inhalte der einzelnen Initiativen sowie die Analyse der Unterschiede, Gemeinsamkeiten und Zusammenhänge beinhalten. Um die Zusammenhänge ausreichend darzustellen, wird ergänzend zur Darstellung der Inhalte besonderer Wert auf die Erfassung der Rahmenbedingungen und der Form der Initiativen gelegt.

Abgrenzungen der zu untersuchenden Initiativen ergeben sich aus der dem Projekt zugrundeliegenden Auftragsbeschreibung sowie durch die Festlegung der Vergleichskriterien. Über die geographische Einschränkung hinaus begrenzt die ausschließliche Betrachtung staatlicher respektive öffentlicher und privat-öffentlicher Initiativen die Untersuchung. Der öffentliche Beitrag kann dabei in der eigentlichen Umsetzung der Maßnahmen, der (Teil-) Finanzierung eines Projekts, der Bereitstellung einer Plattform oder der lediglich ideellen Unterstützung liegen. Dementsprechend variieren die Inhalte der in Frage kommenden Initiativen. Dem Staat stehen hier unter anderem als Instrumente Kampagnen, technische Unterstützungsleistungen, Frühwarnsysteme und gesetzliche Regelungen sowie Gutscheine zur Verfügung.

Des Weiteren sind im Rahmen der Untersuchung nur Initiativen von Interesse, die sich an die mittelständische Wirtschaft richten. Dies beinhaltet die Möglichkeit, auch Initiativen zu berücksichtigen, die eine wesentliche Bedeutung für KMU haben könnten. Da das BMWi der Adressat der Studienergebnisse ist und, wie oben ausgeführt, die Initiativen des Ressorts

den Referenzrahmen des Vergleichs darstellen, empfiehlt sich eine Einschränkung dahingehend, dass nur Initiativen in den Vergleich eingehen, die KMU explizit als Zielgruppe ansprechen und diesen einen Mehrwert bieten.

Abschließend kommen nur Initiativen im Bereich der IT-Sicherheit in Betracht. Damit stellt sich die Frage nach der Definition von IT-Sicherheit. Nach Definition des BSI beschäftigt sich IT-Sicherheit „an erster Stelle mit dem Schutz elektronisch gespeicherter Informationen und deren Verarbeitung“ (BSI 2008). An gleicher Stelle weist das BSI darauf hin, dass „die elektronische Verarbeitung von Informationen in nahezu allen Lebensbereichen allgegenwärtig ist und somit die Unterscheidung, ob Informationen mit Informationstechnik, mit Kommunikationstechnik oder auf Papier verarbeitet werden, nicht mehr zeitgemäß ist, weshalb der Begriff Informationssicherheit statt IT-Sicherheit (…) umfassender und besser geeignet“ sei. Eine zu enge, auf technische Belange wie Systeme, Infrastruktur, Applikationen und anderes konzentrierte Abgrenzung würde auch nach den derzeitigen Erkenntnissen der Forschung dem Problem und so dem Ziel der Studie nicht gerecht. Daher orientiert sich die vorliegende Untersuchung an dem Begriff der Informationssicherheit. So wird gewährleistet, dass alle Initiativen, die einen Beitrag zur Sicherheit elektronisch digitalisierter Informationen in KMU leisten, in die Analyse eingehen.

Die Europäische Kommission (2006) definiert drei Kategorien von KMU: Kleinstunternehmen, Kleinunternehmen und mittlere Unternehmen. Ausschlaggebende Faktoren für die Kategorisierung sind die Zahl der Mitarbeiter und entweder Umsatz oder Bilanzsumme (siehe Tabelle 1).

Unternehmenskategorie	**Mitarbeiter**	**Umsatz**	*oder*	**Bilanzsumme**
Mittleres Unternehmen	< 250	≤ 50 Mio. EUR		≤ 43 Mio. EUR
Kleinunternehmen	< 50	≤ 10 Mio. EUR		≤ 10 Mio. EUR
Kleinstunternehmen	< 10	≤ 2 Mio. EUR		≤ 2 Mio. EUR

Tabelle 1: Definition kleiner und mittelständischer Unternehmen laut Europäische Kommission

2.2 Methodisches Vorgehen

In Einklang mit den zuvor beschriebenen Zielen der Studie stehen die Erfassung und der Vergleich von Initiativen zur Informationssicherheit in KMU in europäischen Ländern und in den USA im Mittelpunkt des Projekts und definieren ergo auch die eingesetzte Methodik und Struktur. Das Projekt wurde in drei übergeordneten Phasen durchgeführt: Die erste Phase diente der Vorbereitung, die zweite Phase beinhaltete die eigentliche Erfassung und Auswertung der Initiativen und in der dritten Phase schließlich wurden die Ergebnisse aufbereitet und Handlungsempfehlungen für den Auftraggeber abgeleitet. Abbildung 1 bietet einen Überblick über die Projektphasen. Eine detaillierte Darstellung der Projektschritte und der eingesetzten Methodik folgt in den Abschnitten 2.2.1 bis 2.2.3.

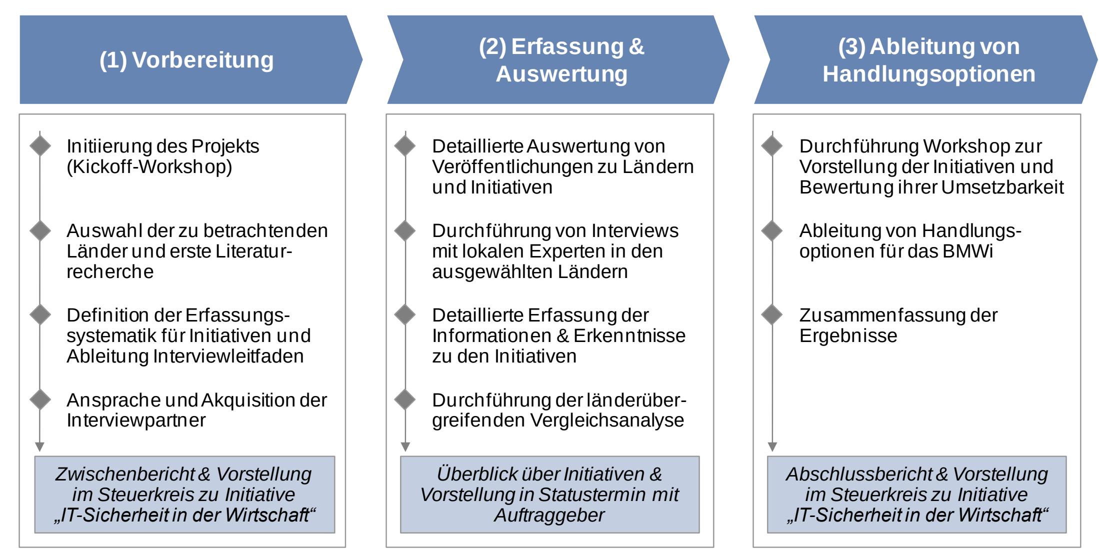


Abbildung 1: Vorgehen im Projekt (vereinfachte Darstellung)

2.2.1 Projektphase 1: Vorbereitung

Der Fokus innerhalb der Projektinitiierung galt der Abstimmung zwischen BMWi und den Auftragnehmern. Dabei wurden im Rahmen des Kickoff-Workshops die Projektziele konkretisiert und der Umfang des Projektes klar definiert.

Am Beginn des Projektes stand die Auswahl zu untersuchender Länder innerhalb der EU. Voraussetzung für die Auswahl eines Landes war, dass erstens – und vor allem – Initiativen in dem jeweiligen Land unter Beteiligung des Staates existierten. Darüber hinaus war es zweitens erstrebenswert, dass die betreffenden Länder zumindest in Ansätzen mit ähnlichen Rahmenbedingungen wie die Bundesrepublik Deutschland konfrontiert waren. Diesen beiden Anforderungen wurde Rechnung getragen, indem die EU-Länder auf Basis von quantitativen und qualitativen Auswahlkriterien hinsichtlich geeigneter Merkmale verglichen wurden. Für die quantitative Beurteilung der Länder wurden insgesamt neun Kriterien herangezogen, die verschiedene, im Kontext der Informationssicherheit in KMU besonders relevante Bereiche abdecken (vgl. dazu Kapitel 3). Die Daten zur Beurteilung der Länder wurden sowohl der Datenbank von Eurostat als auch dem Digital Agenda Scoreboard der Europäischen Kommission entnommen.

Auf Basis der endgültigen, mit dem BMWi abgestimmten Länderauswahl konnte im nächsten Untersuchungsschritt die Recherche der Literatur und Informationsquellen mit explizitem Bezug zu den jeweiligen Ländern durchgeführt werden. Obgleich bereits eine umfangreiche Literaturdatenbank vorhanden war, wurden zur Vervollständigung länderspezifische Publikationen und andere Informationsquellen zur Bedeutung der Informationssicherheit in dem jeweiligen Land, zum Stand derselben in KMU, zu den Gründen mangelnder Informationssicherheit sowie den Details über Initiativen zur Verbesserung der Informationssicherheit in KMU recherchiert. Die Rechercheergebnisse wurden dann systematisch mittels eines Literaturverwaltungs- und Wissensmanagementprogramms katalogisiert und ausgewertet.

Außer den so gesammelten ersten Eindrücken lieferte die Recherche des Weiteren wichtige Hinweise zu den bereits existierenden Initiativen in den Ländern, anhand der die Definition des Kriterienkatalogs ergänzt werden konnte. Bei diesem handelt es sich um eine umfangreiche Liste von Merkmalen, mit denen sich die zu erfassenden Initiativen systematisch und möglichst detailliert beschreiben lassen. Diese Systematisierung erleichterte nicht nur die

Erfassung, sondern ermöglichte überhaupt erst den Vergleich zwischen den Initiativen. Des Weiteren konnten auf Grundlage der Recherche bereits Multiplikatoren identifiziert werden, die im Folgenden als Interviewpartner in Frage kamen, wobei sich außerdem die globale Infrastruktur und Vernetzung der Detecon International und ihres Mutterkonzerns, der T-Systems International, als sehr hilfreich erwiesen hatte.

Die bis hierhin gewonnenen Erkenntnisse sowie die erarbeitete Systematik zur Durchführung der zweiten Phase sind in den Zwischenbericht eingegangen, der neben der Dokumentation der ausgeführten Arbeiten die Grundlage für ein gemeinsames Verständnis über die weiteren Schritte ermöglichen sollte.

2.2.2 Projektphase 2: Erfassung und Auswertung

Im Anschluss an den Zwischenbericht erfolgte im ersten Schritt die Erfassung anhand der Auswertung von Veröffentlichungen über Initiativen zur Informationssicherheit in den zu untersuchenden Ländern. Zu diesem Zweck wurde mittels der erarbeiteten Kriterien ein Tool programmiert, das die elektronische Erfassung der Informationen der Mitarbeiter in den jeweiligen Ländern in einer Datenbankarchitektur erlaubte. Auf diese Weise wurde das Grundgerüst der Informationen geschaffen, aus dem sich nicht zuletzt die weitergehenden Fragen ergeben haben, die Gegenstand der nachfolgenden Interviews waren. Interviews bieten durch das Fehlen vorgegebener Antwortkategorien die Möglichkeit, alle Aspekte eines Sachverhalts unverfälscht aufzunehmen. Allerdings wird damit auch die Vergleichbarkeit der Interviewergebnisse erschwert. Aus diesem Grund wurde im Vorfeld der geplanten Interviews der jeweilige Interviewverlauf mit Hilfe eines Gesprächsleitfaden strukturiert, der gewährleistete, dass die Ergebnisse konsistent zur vorherigen datenbankgestützten Erfassung blieben. Das Interview erhielt so den Charakter eines relativ freien Gespräches, das sich dennoch auf die bedeutsamen Fragen der Untersuchung fokussierte. Um die Individualität der Interviews zu wahren und gleichzeitig länderübergreifend vergleichbare Aussagen treffen zu können, wurden die Interviews in der Landessprache oder wahlweise in Englisch geführt. Mit Abschluss der Interviews stand die vollständige Datengrundlage für die Vergleichsanalyse zur Verfügung. An dieser Stelle zeigte sich der Mehrwert der in der ersten Phase ausgearbeiteten Kriterien, die eine detaillierte Auswertung der Gemeinsamkeiten, Unterschiede und Zusammenhänge der unterschiedlichen Initiativen erlaubten.

2.2.3 Projektphase 3: Ableitung von Handlungsoptionen

Die Ergebnisse der Vergleichsanalyse gingen zu Beginn der dritten Phase zur Diskussion in den Workshop ein, der in Abstimmung mit dem BMWi die Möglichkeit eröffnen sollte, einen weiteren Teilnehmerkreis in das Projekt einzubinden, um die Ergebnisse zu validieren und gegebenenfalls weitere Anregungen aufzunehmen. Hierfür wurden neben deutschen Experten auch Repräsentanten zweier ausländischer Initiativen eingeladen, die einen wertvollen Beitrag zu einer umfassenden Diskussion leisten konnten. Die so ergänzten Ergebnisse wurden anhand einer Zusammenfassung und Priorisierung zur Diskussion mit dem BMWi aufbereitet. Hieraus resultierten schließlich die Empfehlungen, die zusammen mit der Dokumentation der Projektarbeiten Eingang in den Bericht finden.

3 Auswahl der untersuchten Länder

Im folgenden Kapitel wird die Auswahl der EU-Länder vorgestellt. Neben den ausgewählten europäischen Ländern waren die USA als Untersuchungsgegenstand durch den Auftraggeber gesetzt. Zur Unterstützung der Auswahl wurde als zentrale Datenquelle die Datenbank des statistischen Amts der Europäischen Union (Eurostat), insbesondere die gesonderte Erhebung zur Sicherheit im Internet aus dem Jahr 2010, herangezogen. Diese Daten bieten die umfangreichste uns bekannte Informationsbasis zur Informationssicherheit von Unternehmen. Einschränkend bleibt nur zu erwähnen, dass die Antworten zu den speziellen Fragen zur IT in nur wenigen Ländern für Unternehmen mit weniger als zehn Beschäftigten verfügbar sind, so dass in diesen Fällen ein Vergleich für Kleinstunternehmen nicht möglich war.

Zu Beginn stellt sich die Frage, welche Länder wirtschaftlich mit Deutschland vergleichbar wären. Prinzipiell stellen Kleinstunternehmen in allen Ländern die mit Abstand größte Gruppe dar. Allerdings ist der Anteil dieser Gruppe in Deutschland, wie Abbildung 2 zeigt, im Vergleich zu den anderen Ländern deutlich kleiner.

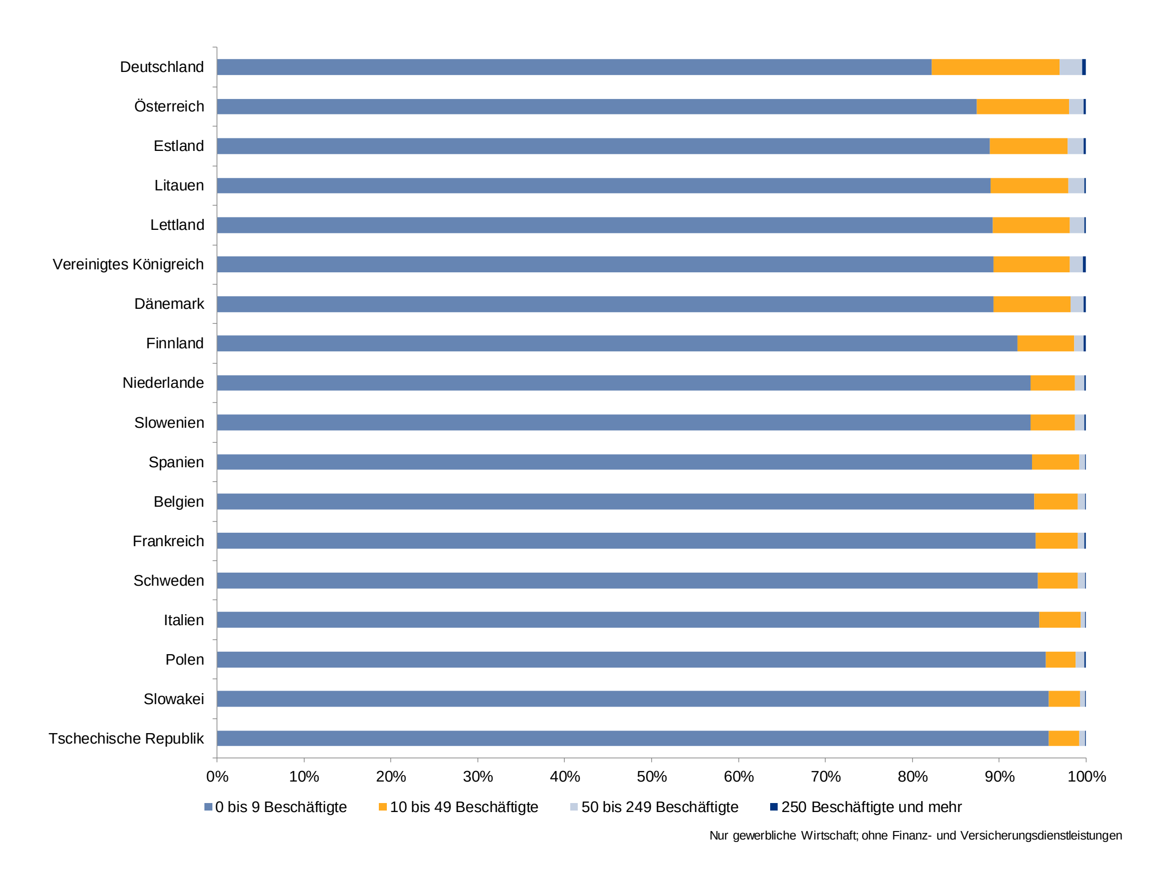


Abbildung 2: Anteil der Unternehmen nach Beschäftigtengrößenklassen (2010)

Der hohe Industrialisierungsgrad Deutschlands zeigt sich nicht nur in der Zahl der Unternehmen mit mehr als 10 Beschäftigten, sondern auch in dem relativ hohen Anteil kleinerer und größerer Mittelständler mit 10 bis 249 Beschäftigten. Insbesondere in dieser Gruppe finden sich eine Reihe der „Hidden Champions“, die oftmals technologisch führend sind und so einen großen Beitrag zum wirtschaftlichen Erfolg Deutschlands leisten. Zwar weist kein Land eine ähnlich starke mittelständische Struktur auf, dennoch zeichnet sich mit den sechs

Deutschland nachfolgenden Ländern eine Gruppe ab, die sich von den verbleibenden Ländern abgrenzt. Dass zu dieser Gruppe auch die baltischen Staaten gehören, eröffnet für die weitere Analyse eine Option, mit der nicht unbedingt zu rechnen war. Die Bedeutung größerer Unternehmen für die Beschäftigungs- und somit auch die Wirtschaftspolitik wird noch deutlicher durch die in Abbildung 3 dargestellte Verteilung der Beschäftigten.

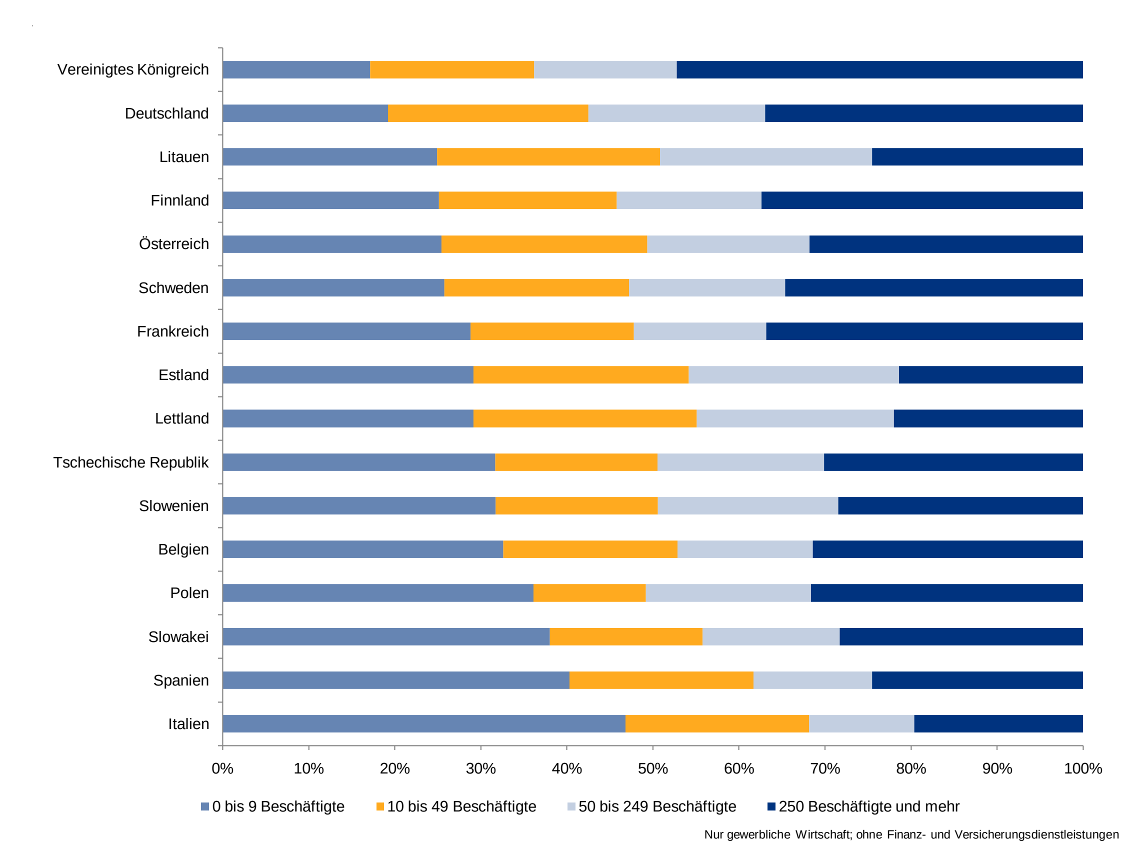


Abbildung 3: Anteil der Beschäftigten nach Beschäftigtengrößenklassen (2010)[6]

Die Änderungen in der Rangfolge lassen sich in erster Linie auf den sehr hohen Anteil von Großunternehmen in Großbritannien, Finnland, Schweden und Frankreich zurückführen. Zwar sind diese Unternehmen auch in Deutschland zahlreich vertreten, der im Vergleich aber dennoch hohe Anteil mittelständischer Unternehmen unterstreicht die Bedeutung des Mittelstands für die deutsche Wirtschaft. Bis hierhin bleibt festzuhalten, dass Großbritannien sowie Österreich, aber eben auch die baltischen Staaten durchaus geeignete Vergleichsländer sein könnten.

Eine weitere Möglichkeit zur Identifikation geeigneter Länder besteht darin, zu fragen, inwieweit das jeweilige Land für Cyberattacken attraktiv ist beziehungsweise mangelnde Informationssicherheit wirtschaftliche Schäden nach sich ziehen könnte, womit ein entsprechender Handlungsdruck verbunden sein sollte. Zu diesem Zweck gibt Abbildung 4 die Anteile der Unternehmen im Spitzentechnologiesektor wieder.

---

[6] Für Dänemark und die Niederlande waren zu diesem Merkmal keine Daten verfügbar.

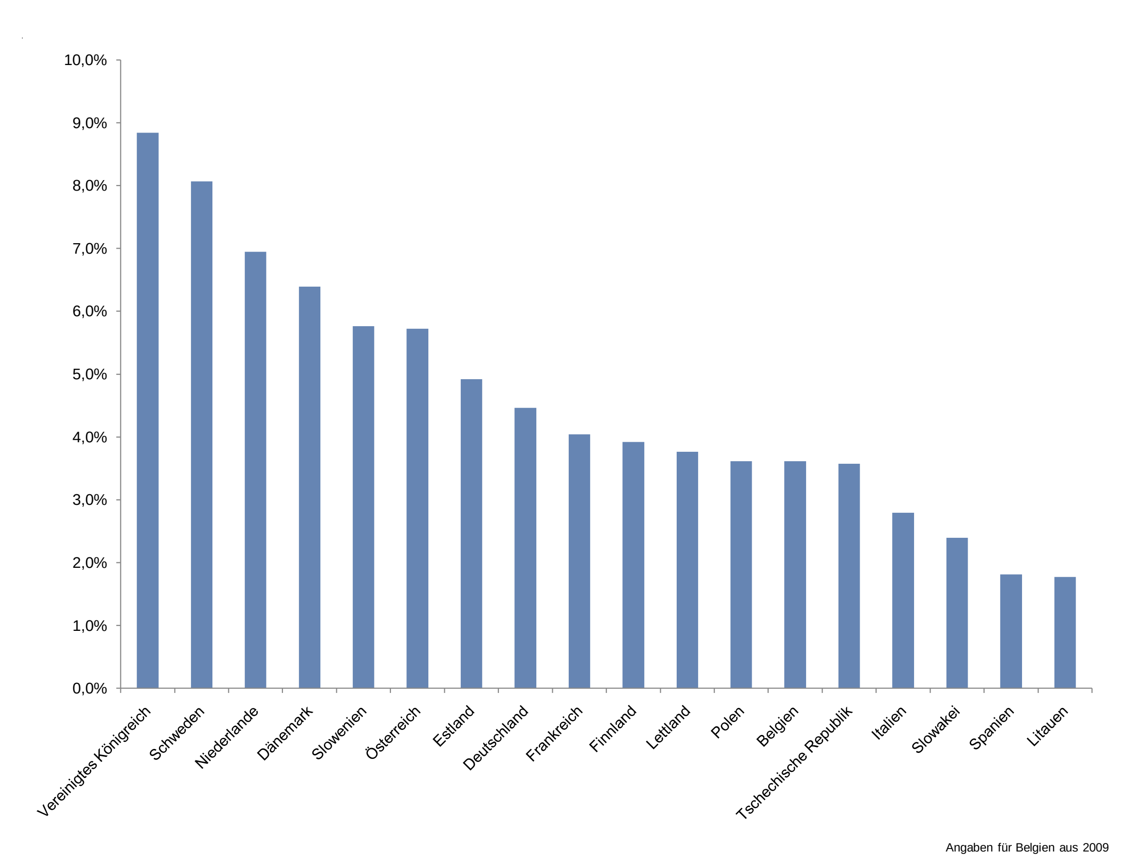


Abbildung 4: Anteile der Unternehmen (ab 10 Beschäftigten) mit hohem Technologieniveau bzw. wissensintensiven Dienstleistungen (2010)

Unter Berücksichtigung der vorangegangenen Statistiken sind hier vor allem Großbritannien Österreich, Schweden und Estland von Interesse. Inwieweit die Niederlande, Dänemark und Slowenien gegebenenfalls auch Untersuchungskandidaten sind, muss im Weiteren eruiert werden.

Ebenfalls ein stärkeres Interesse, Initiativen zur IT-Sicherheit zu implementieren, sollten die Länder haben, in denen der elektronische Geschäftsverkehr eine hohe Relevanz besitzt. Entsprechende Merkmale sind das Internetbanking und der Onlinekauf, deren Bedeutung aus Abbildung 5 hervorgeht.

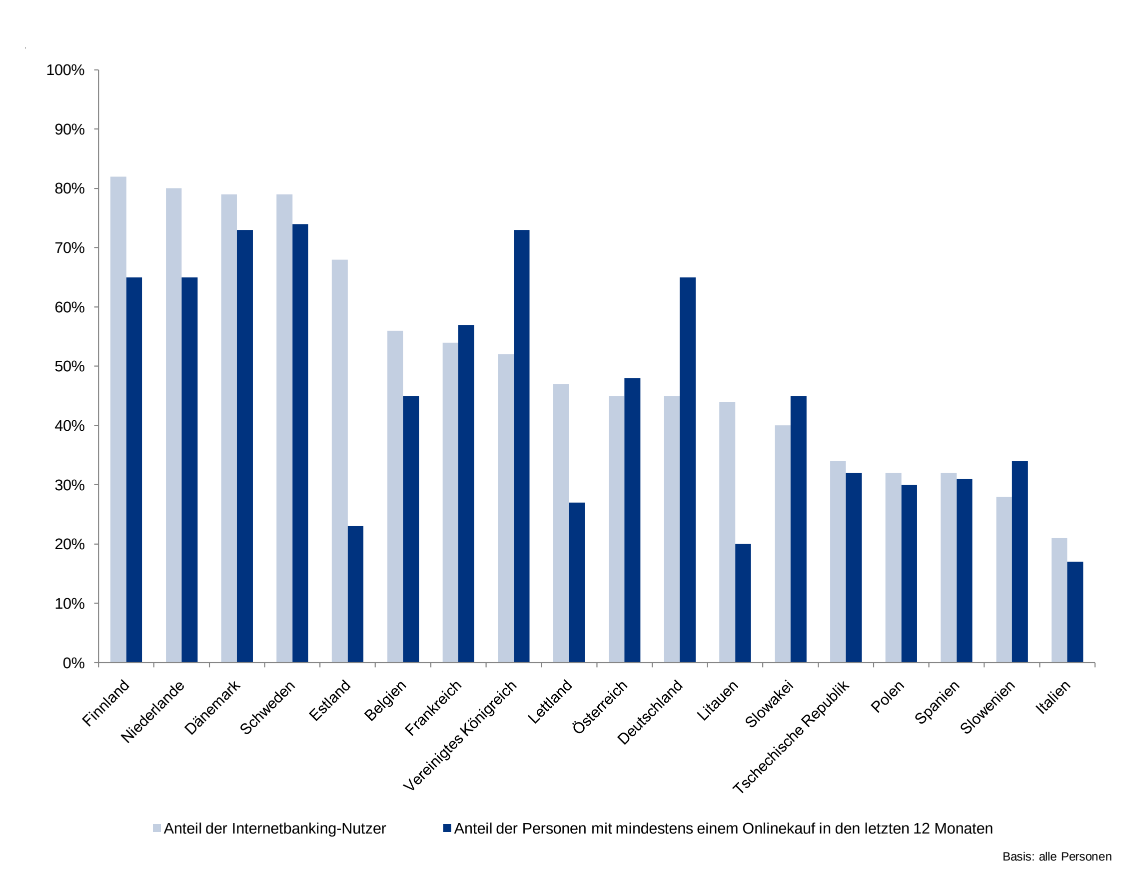


Abbildung 5: Nutzung von Internetbanking und E-Commerce durch die Verbraucher (2012)

In Bezug auf das äußerst sensible Internetbanking scheinen doch noch viele Bundesbürger zurückhaltender zu sein als etwa die Verbraucher in den skandinavischen Ländern, den Beneluxstaaten, den baltischen Staaten sowie Großbritannien und Frankreich. Etwas zugeneigter sind Deutsche dem Onlineshopping, wobei hier Großbritannien, die skandinavischen Länder und die Niederlande ähnlich oft Gebrauch vom Internet für ihre Einkäufe machen.

Ein weiterer Grund für ein Land, sich mit dem Thema IT-Sicherheit verstärkt auseinanderzusetzen, liegt in der Wahrscheinlichkeit eines – absichtlichen oder unabsichtlichen – unerwünschten Kontakts per Internet, die mit dem zunehmendem Anteil der Beschäftigten, die über einen an das Internet angeschlossenen Computer verfügen, steigen dürfte.

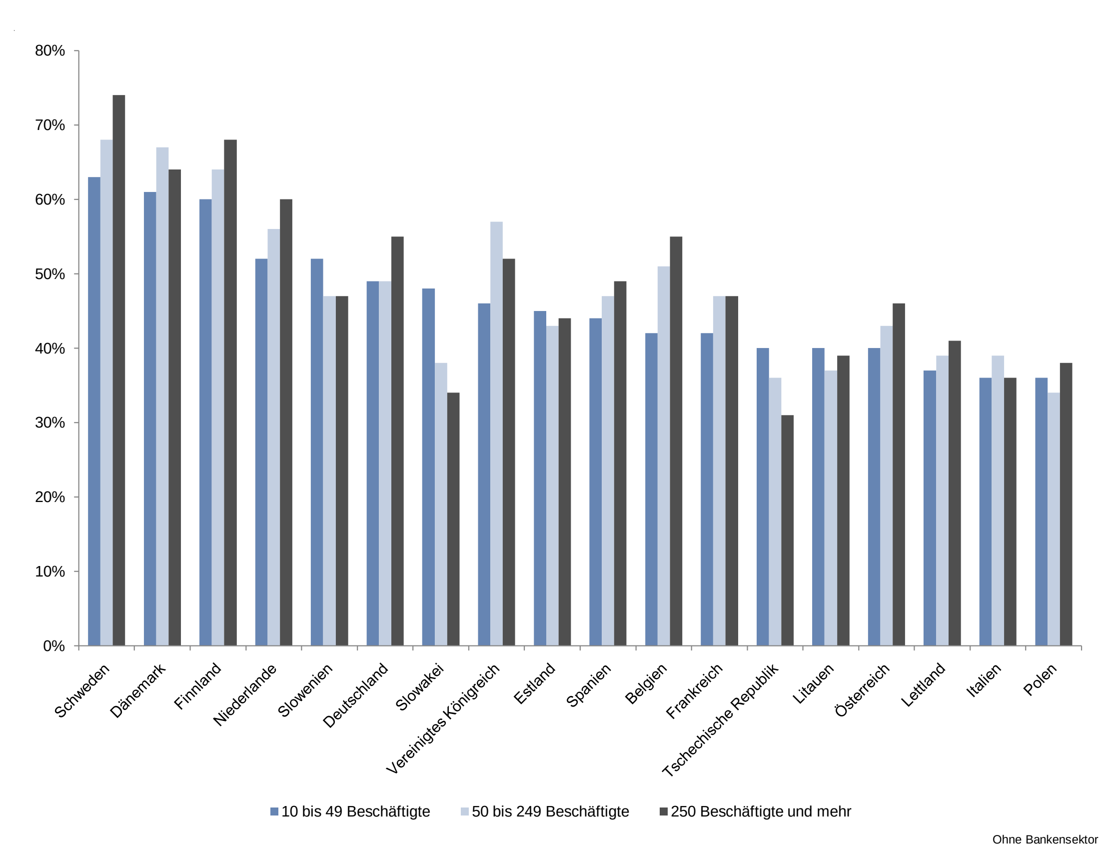


Abbildung 6: Anteil der Beschäftigten, die an das Internet angeschlossene Computer nutzen (2012)

Auch wenn mittlerweile in allen Ländern ein großer Teil der Beschäftigten für ihre Arbeit auf das Internet zugreifen, so fallen in Abbildung 6 dennoch vor allem die skandinavischen Länder ins Auge, die sich unabhängig von der Unternehmensgröße in der Spitze von den anderen Ländern abgrenzen.

Eine wesentliche Frage für den Vergleich mehrerer Länder ist, inwieweit nicht nur die Wahrscheinlichkeit eines Sicherheitsvorfalls besteht, sondern wie oft ein solcher tatsächlich eingetreten ist. Hier findet sich Deutschland in Abbildung 7 in der Gruppe der Länder, deren Unternehmen in der Befragung nur vergleichsweise wenige Sicherheitsvorfälle angaben.

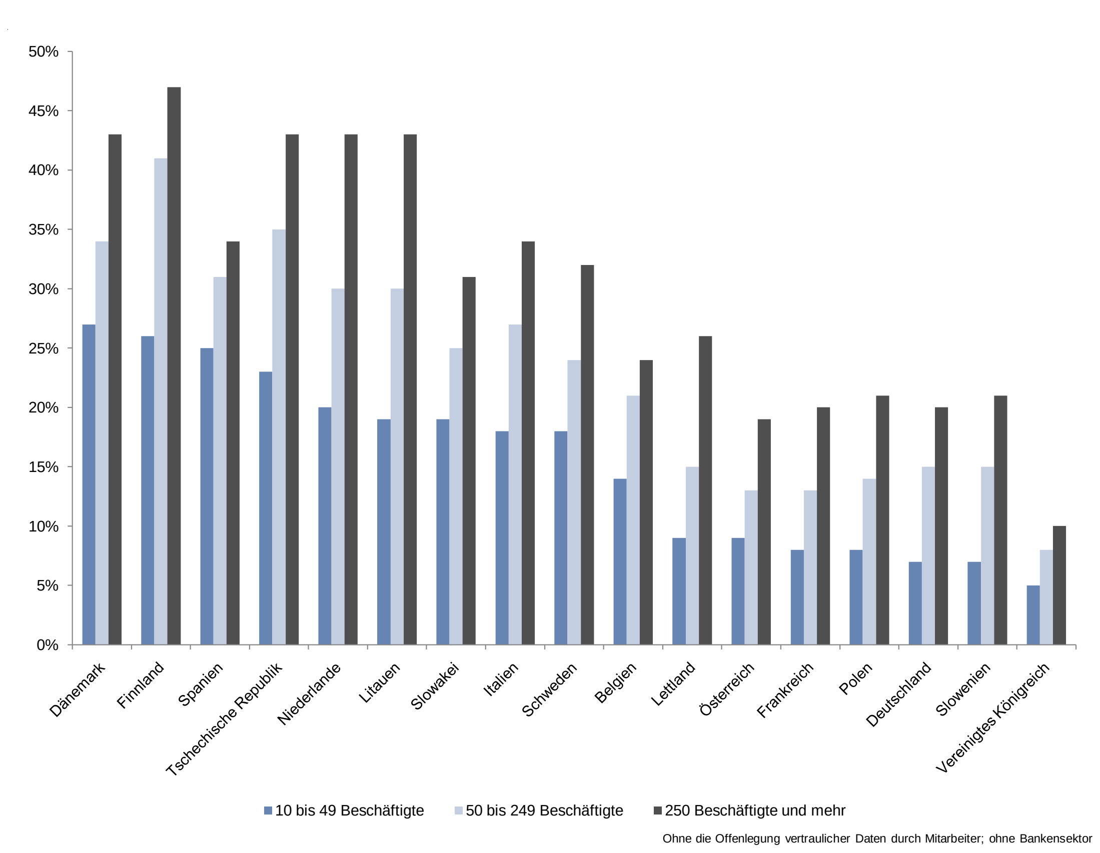


Abbildung 7: Anteile der Unternehmen mit Sicherheitsproblemen im Berichtsjahr (2010)[7]

Einen Handlungsbedarf haben sicherlich Länder mit relativ vielen Sicherheitsvorfällen, die unter Umständen seit 2010 auch staatliche Initiativen zur Folge hatten. Inwieweit Länder mit nur wenigen berichteten Sicherheitsvorfällen für die Untersuchung von Interesse sind, ist schwer einzuschätzen. Zum einen könnte ein geringer Anteil auch daraus resultieren, dass die betreffenden Unternehmen den Vorfall gar nicht bemerkten. Zum anderen existiert in solchen Ländern nicht unbedingt ein Anreiz, Initiativen zur Reduktion von Sicherheitsvorfällen zu starten. Lediglich in der Annahme, entsprechende Initiativen wurden bereits vor 2010 eingeleitet, könnten diese Länder für die Untersuchung interessant erscheinen lassen.

Einen Vorteil im Hinblick auf die Informationssicherheit haben aller Wahrscheinlichkeit nach die Länder, in denen der elektronische Austausch mit der Verwaltung bei Unternehmen Vertrauen genießt. Es ist anzunehmen, dass der Staat sich dieses Vertrauen zuvor verdient hat. Für Deutschland offenbart Abbildung 8 angesichts von rund 30 Prozent misstrauischer Unternehmen – über alle Größenklassen hinweg – ein noch erhebliches Optimierungspotenzial.

[7] Für Estland waren zu diesem Merkmal keine Daten verfügbar.

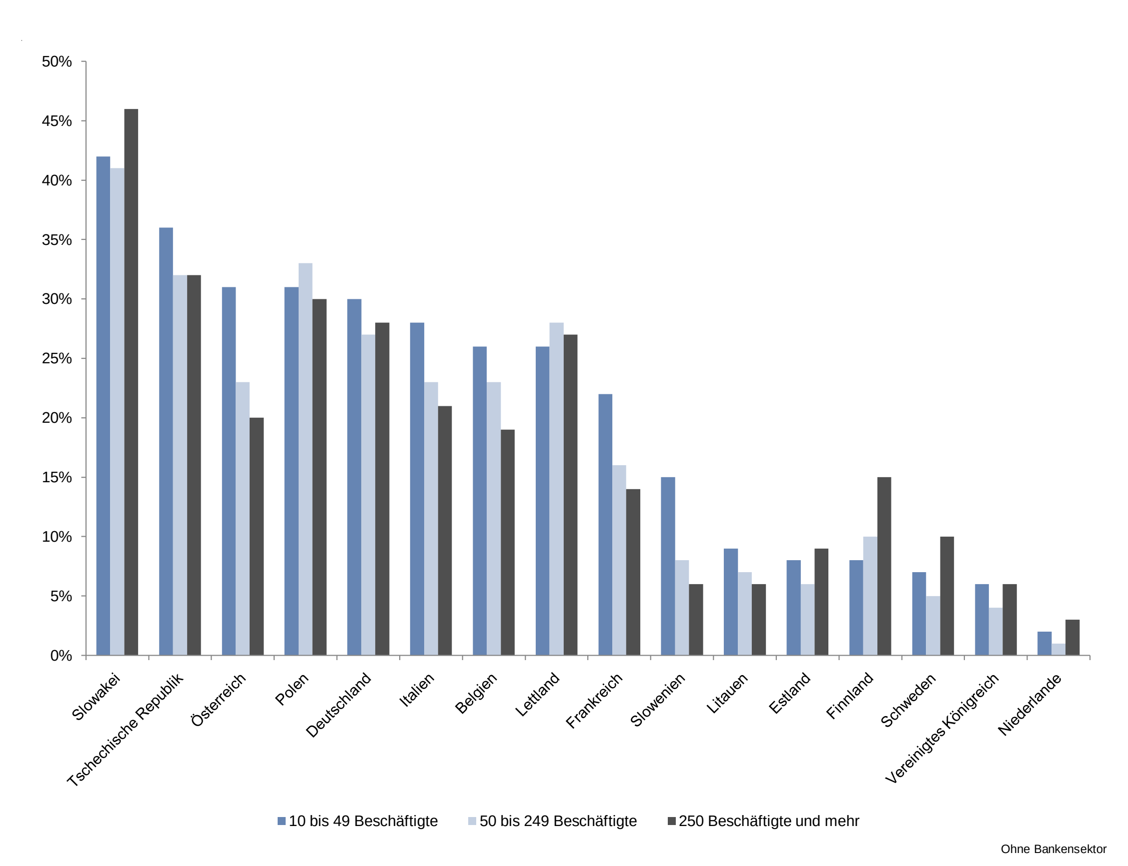


Abbildung 8: Anteile der Unternehmen mit Bedenken bezüglich der Vertraulichkeit und Sicherheit der Daten in der Abwicklung elektronischer Verwaltungsvorgänge (2011)[8]

Auf Basis dieser Auswertung kommen für die Vergleichsanalyse wiederum baltische und skandinavische Staaten sowie Großbritannien und die Niederlande in Betracht. Insbesondere Letztere könnten wertvolle Hinweise liefern für den sicheren Austausch von Daten zwischen Unternehmen und Verwaltung.

Die folgenden fünf Abbildungen geben den Stand der Informationssicherheit in Unternehmen anhand ausgesuchter Merkmale wieder. Dabei ist davon auszugehen, dass Länder, in denen Unternehmen einen hohen Sicherheitsstand aufweisen, eher für den Zweck dieser Studie geeignet sind.

Ein Merkmal, das Hinweise auf die grundlegende Einstellung zu Informationssicherheit erlaubt, ist die Existenz einer IKT-Politik. Abbildung 9 zeigt zunächst einmal einen beträchtlichen Unterschied zwischen kleinen, mittleren und großen Unternehmen.

[8] Für Spanien und Dänemark waren zu diesem Merkmal keine Daten verfügbar.

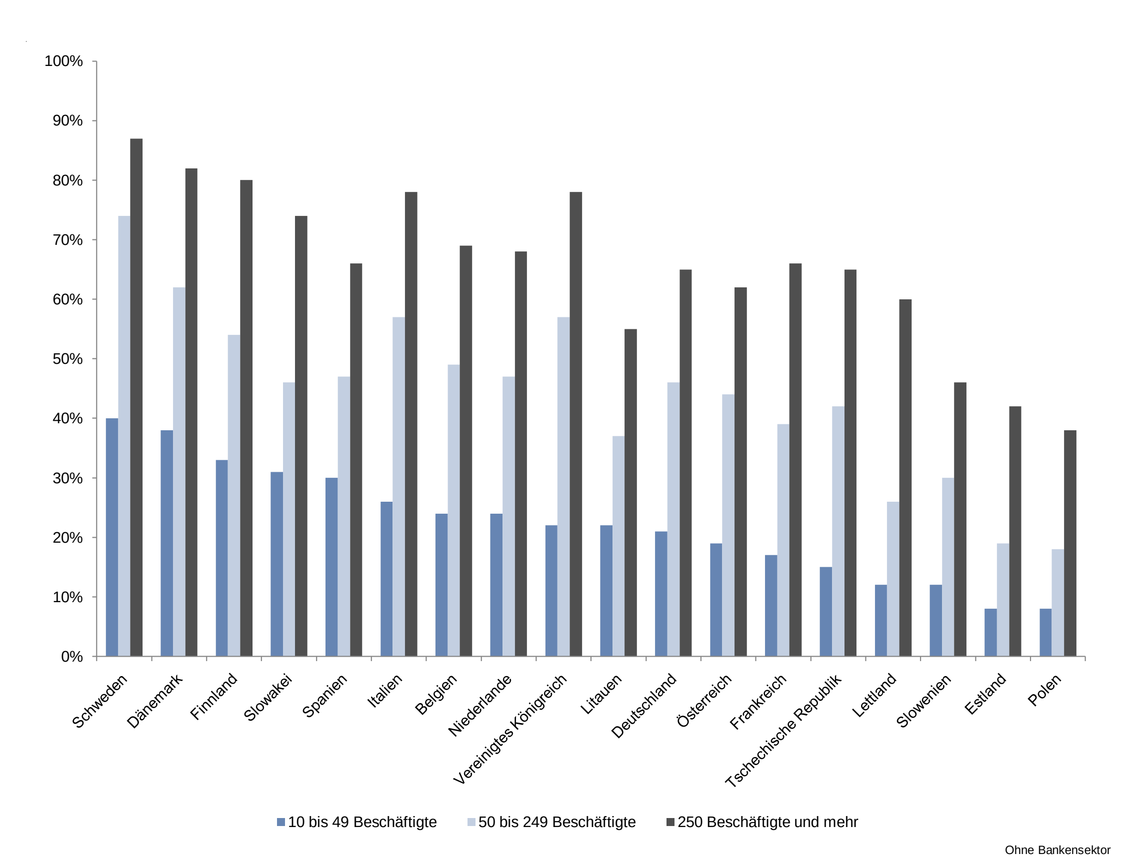


Abbildung 9: Anteile der Unternehmen mit einer formell festgelegten Sicherheitspolitik einschließlich eines Konzeptes mit regelmäßiger Überprüfung (2010)

Besonders groß ist die Diskrepanz in Italien und Großbritannien. Jedoch auch in den Ländern, in denen Kleinunternehmen eher über eine IKT-Politik verfügen, bleibt der Abstand erheblich. Mit Blick auf die Kleinunternehmen erreichen wiederum die skandinavischen Länder die besten Werte. Aber auch die Slowakei, Spanien und Italien sind – wenn auch unerwartet – im vorderen Drittel zu finden.

Ebenso selten wie Kleinunternehmen eine IKT-Politik formulieren, protokollieren sie die Vorgänge auf ihren Systemen zur Analyse von Sicherheitsproblemen, wie Abbildung 10 illustriert. Der Grund dafür liegt sicherlich nicht zuletzt in der speziellen Ausbildung, die für eine Verwendung solcher Protokolle erforderlich ist. Während große Unternehmen entsprechende Fachleute in der hauseigenen IT-Abteilung haben, müssen kleine Unternehmen eine solche Expertise in der Regel über externe Dienstleister einkaufen.

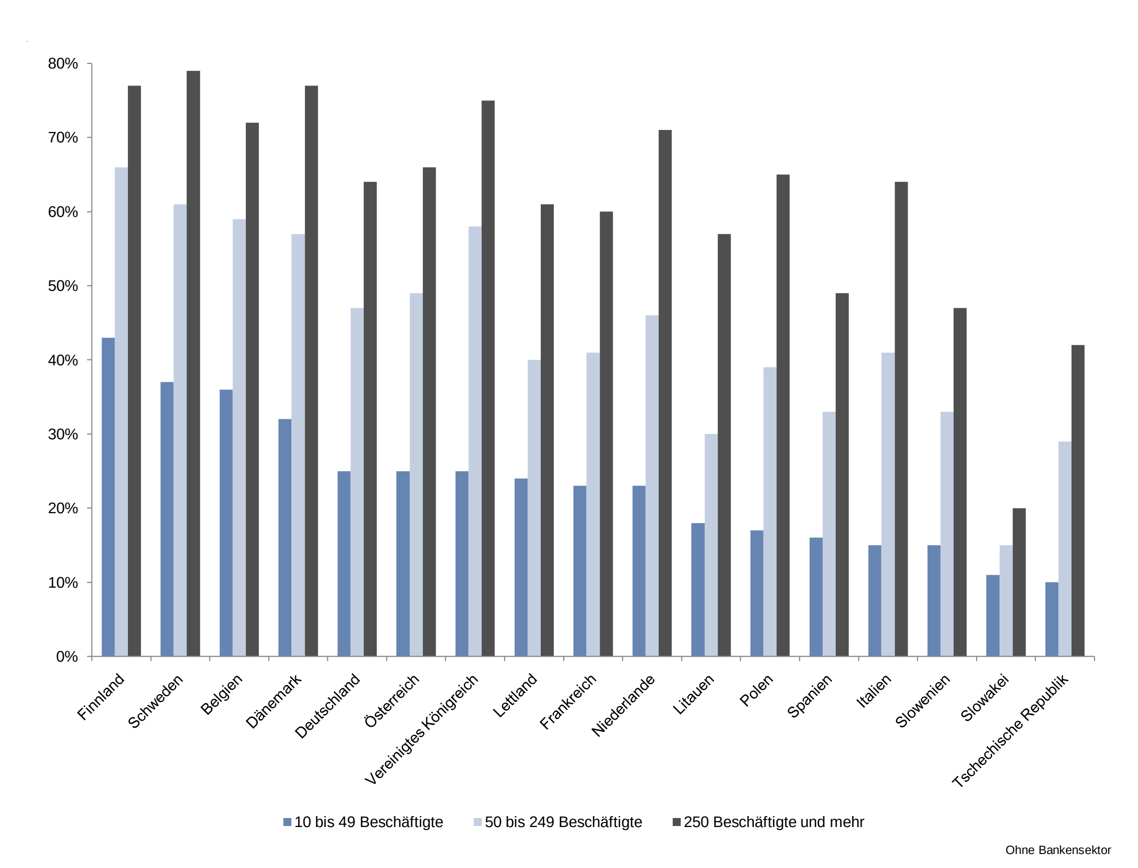


Abbildung 10: Anteile der Unternehmen, die Vorgänge zur Analyse von Sicherheitsproblemen protokollieren (2010)[9]

Die Protokollierung ist üblicherweise Teil einer IKT-Politik. Insofern verwundert es nicht, dass die skandinavischen Länder, ergänzt um Belgien, auch hier die vorderen Plätze belegen. Allerdings haben sich auch Änderungen im Vergleich zur vorherigen Auswertung ergeben. Vor allem erstaunt der Rückfall Spaniens und Italiens in der Rangfolge, da doch offensichtlich ein erheblicher Teil der Unternehmen dort, obwohl eine IKT-Politik im Unternehmen existiert, keine Protokollierung vornehmen.

Ein wichtiges Werkzeug zur Sicherung von Informationen ist die Authentifizierung für den Zugang zu den Unternehmenssystemen. Deutschland rangiert im Hinblick auf dieses Kriterium in Abbildung 11 nur im letzten Drittel. Vor allem kleine Unternehmen schützen ihre Informationen auf diese Weise nur zu wenig mehr als einem Drittel, obwohl bereits strengere Passwortvorgaben ohne signifikanten Mehraufwand ein deutlich höheres Sicherheitsniveau ermöglichen.

[9] Für Estland waren zu diesem Merkmal keine Daten verfügbar.

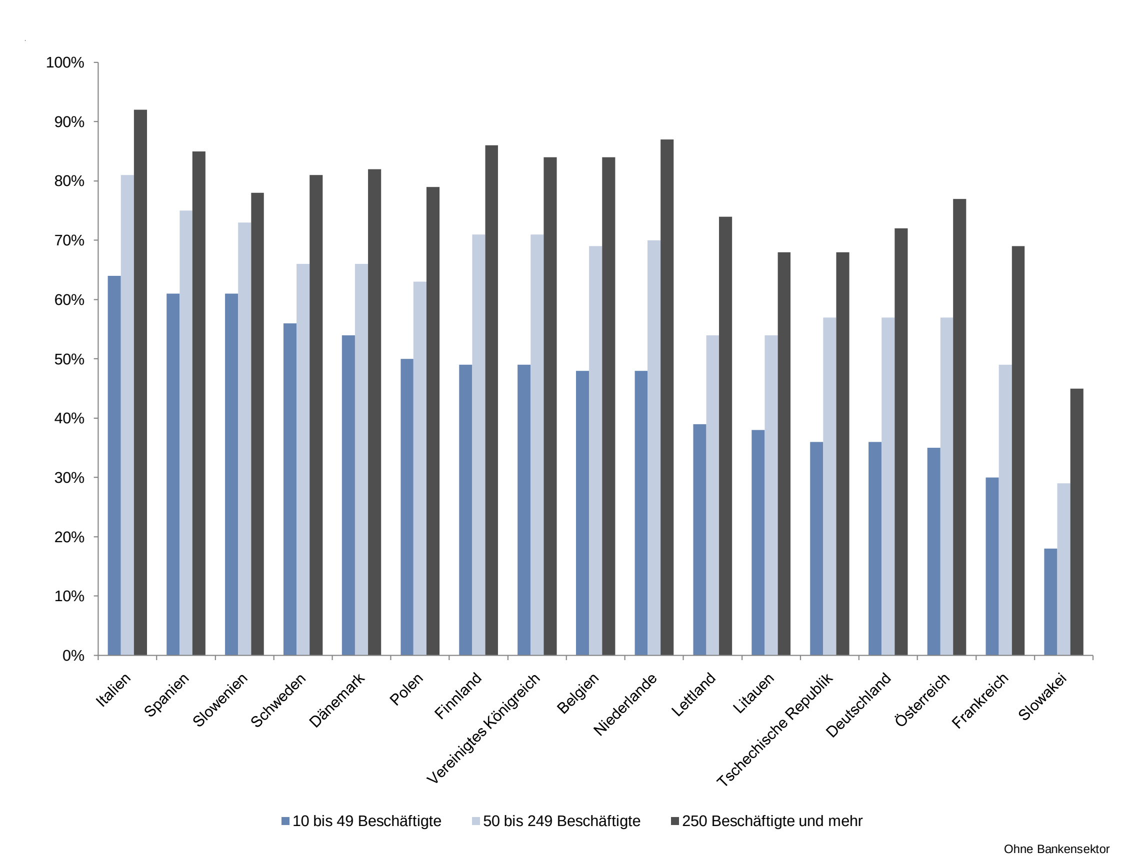


Abbildung 11: Anteile der Unternehmen, die strenge Passwort- Authentifizierung oder Nutzeridentifizierung bzw. -authentifizierung via Hardware-Elemente verwenden (2010)[10]

Vor allem spanische und italienische Unternehmen erhöhen den Schutz ihrer Daten vor unerlaubtem Zugriff auf diese Weise. Allerdings ist der Vorsprung – auch unter Berücksichtigung mittelständischer Unternehmen – gegenüber den nachfolgenden Ländern vergleichsweise klein.

Ebenfalls eine einfache Maßnahme zur Erreichung einer höheren Informationssicherheit stellt die Sicherung der Unternehmensdaten auf externen Servern dar. Jedoch ist ein solches Hosting nicht immer möglich respektive sinnvoll. Erstens bedarf es für diese Lösung einer ausreichend schnellen Internetverbindung. Zweitens muss gewährleistet sein, dass auch die Übertragung sowie die Speicherung den Sicherheitsanforderungen des Unternehmens genügen. Drittens können die Kosten gerade kleine Unternehmen von einer externen Datensicherung abhalten.

[10] Für Estland waren zu diesem Merkmal keine Daten verfügbar.

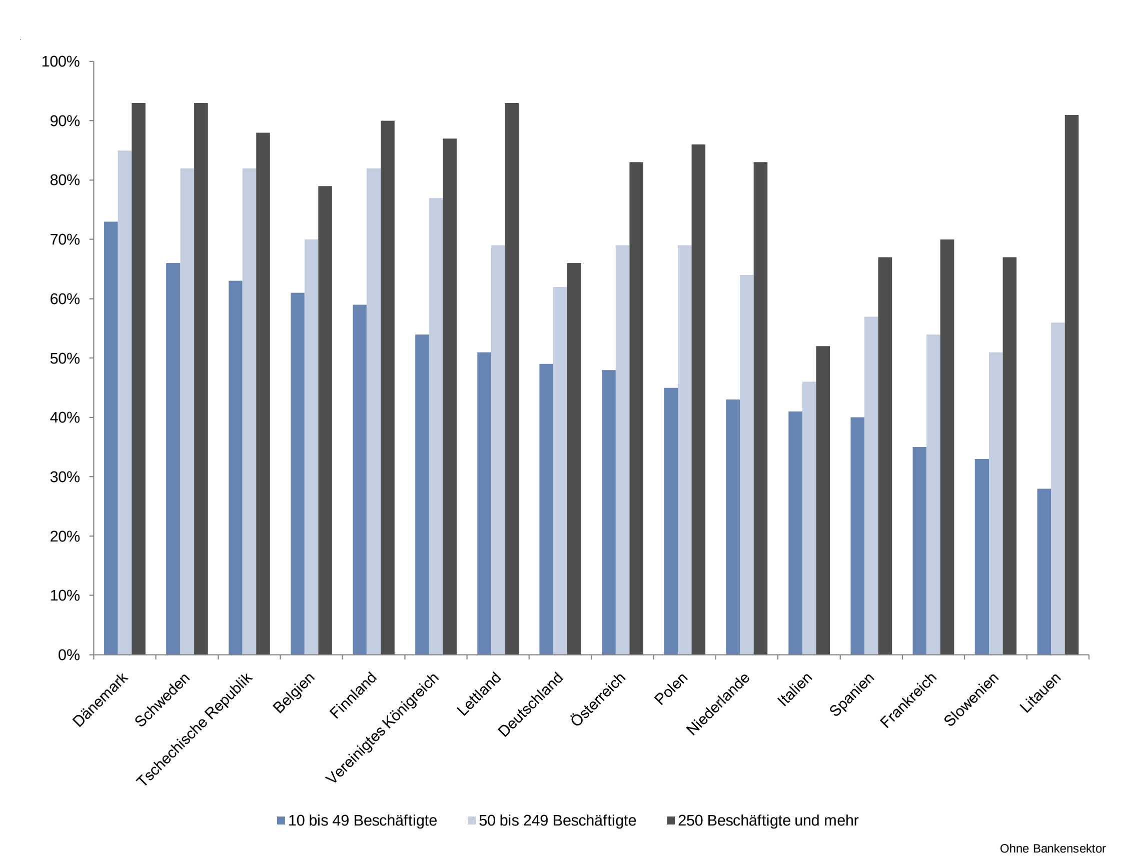


Abbildung 12: Anteile der Unternehmen, die externe Datensicherung verwenden (2010)[11]

Trotz dieser möglichen Hemmnisse nutzen Kleinunternehmen die externe Speicherung im Vergleich zu den anderen bisher erläuterten Instrumenten überraschend ausgiebig. Auffallend in Abbildung 12 ist der von links nach rechts zunehmende Abstand zwischen kleinen und großen Unternehmen. Offensichtlich konnten die Länder im vorderen Drittel, hier wiederum allen voran Dänemark und Schweden, bessere Rahmenbedingungen schaffen.

Die Verschlüsselung von E-Mails ist – wie bereits in der Einleitung erwähnt – ein Stiefkind in deutschen Unternehmen. Allerdings trifft dies in Abbildung 13 nicht nur für Deutschland, sondern auch für die Länder zu, die in anderer Hinsicht ein hohes Sicherheitsniveau aufweisen.

[11] Für Estland waren zu diesem Merkmal keine Daten verfügbar.

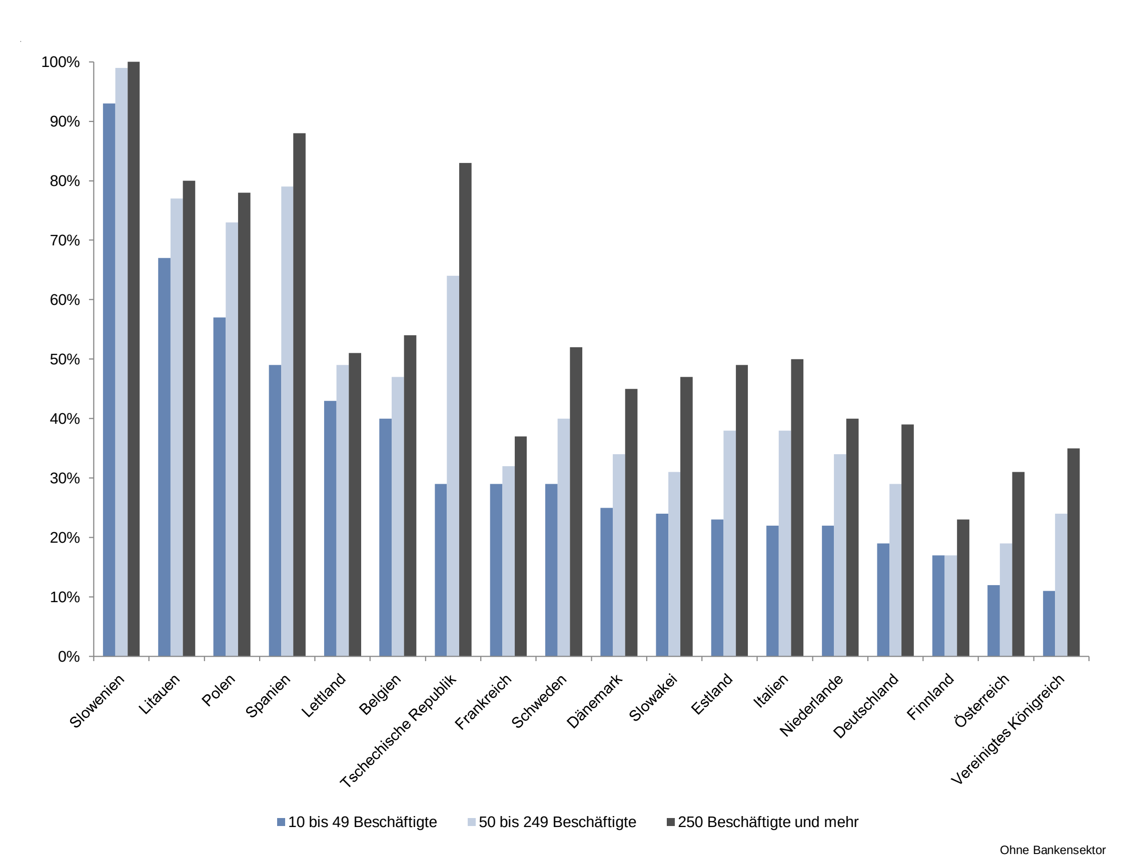


Abbildung 13: Anteil der Unternehmen, die fortschrittliche elektronische Signaturen in ihren Zulieferern- oder Kundenbeziehungen verwenden (2010)

Grob lässt sich eine Zweiteilung in Europa erkennen, die aber vermutlich weniger aus einem grundsätzlich unterschiedlichen Sicherheitsbedürfnis als eher aus den rechtlichen Rahmenbedingungen heraus resultiert. So schreibt das slowenische „Gesetz über den elektronischen Handel und die elektronische Signatur“ nicht nur zur Geltendmachung der Vorsteuer, sondern grundsätzlich „die Verwendung einer sicheren, auf einem qualifizierten Zertifikat beruhenden elektronischen Signatur“ (Europäische Kommission 2010) vor.

Ein Merkmal, das auf einen effizienten Umgang mit dem Thema Informationssicherheit schließen lässt, ist die Inanspruchnahme externer Dienstleister (Ghobakhloo et al. 2011). Wie Abbildung 14 zeigt, ergibt sich die Rangfolge der Länder weniger aus dem Vergleich größerer Unternehmen, als vielmehr aus der Betrachtung der Kleinunternehmen. Während große Unternehmen tendenziell rational auf Basis von Grenzkosten und Grenznutzen Aufträge an Externe vergeben, sind die Entscheidungen kleiner Unternehmen oftmals durch Überschätzung oder Misstrauen verzerrt (Eichfelder und Schorn 2012).

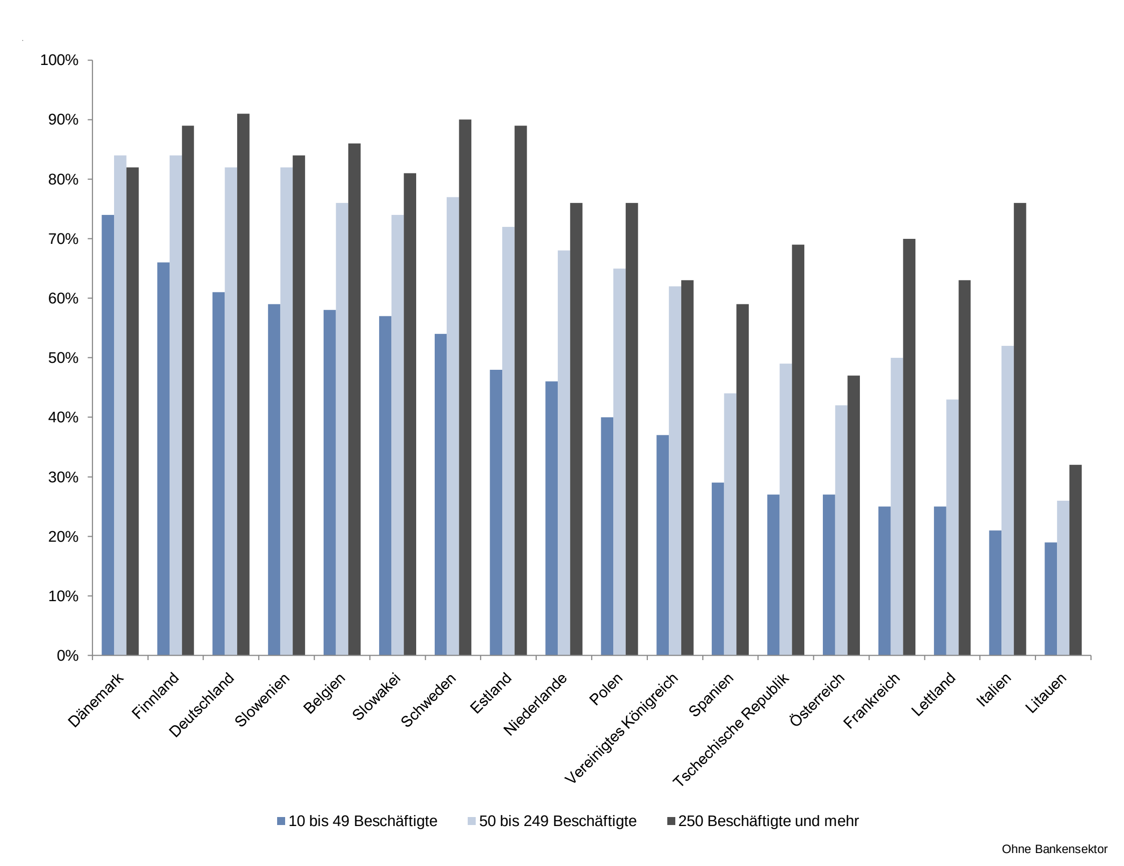


Abbildung 14: Anteile der Unternehmen, die IKT-Aufgaben von externen Auftragnehmern erledigen lassen (2007)

Im internationalen Vergleich lässt sich festhalten, dass deutsche Kleinunternehmen die Vorteile externer Dienstleister zu einem großen Teil bereits 2007 erkannt haben. Sicherlich besteht auch hier noch ein Optimierungspotenzial, auf den ersten Blick sind aber keine Länder erkennbar, die in diesem Punkt besonders vielversprechend wären.

Das letzte Kriterium, anhand dessen die Identifikation interessanter Länder möglich sein könnte, sind die Fortbildungen, die Unternehmen den Mitarbeitern zukommen lassen, die nicht ohnehin in der hauseigenen IT-Abteilung arbeiten. Allerdings kann sich zumindest in Bezug auf die Kleinunternehmen kein Land wirklich empfehlen. In Abbildung 15 fällt vor allem der Unterschied zwischen größeren und kleineren Unternehmen auf, der zwar auch schon in den anderen Auswertungen zu beobachten war, hier jedoch sehr ausgeprägt ist.

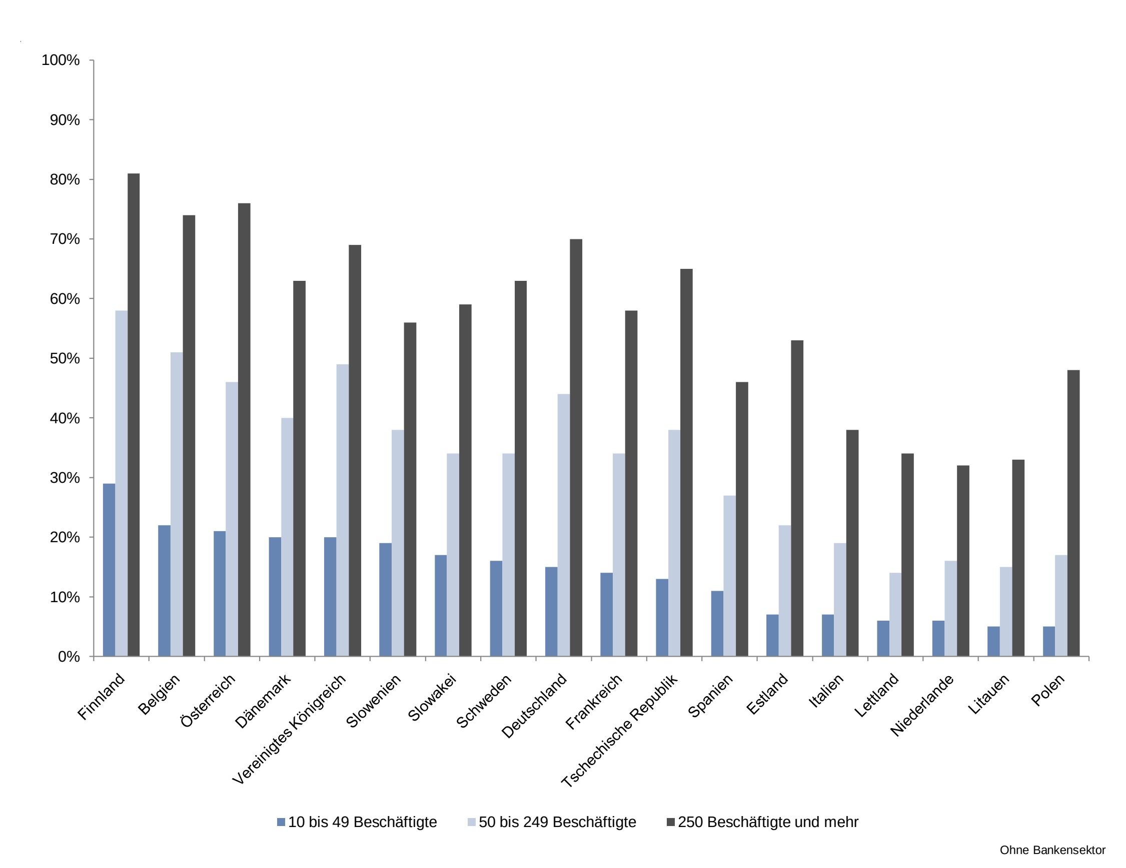


Abbildung 15: Anteile der Unternehmen, die für Nicht-IKT-Beschäftigte IKT-Fortbildungsmaßnahmen durchführten (2012)

Zusammenfassend ergibt der statistische Vergleich einen ersten Überblick zu den Ländern, die in die weitere Untersuchung eingehen könnten. Hierzu gehören die skandinavischen Länder sowie Großbritannien. Darüber hinaus haben sich in Bezug auf einzelne Kriterien aber auch andere Länder als durchaus interessant erwiesen. Um nun an dieser Stelle den Kreis möglicher Kandidaten weiter einzugrenzen, werden im Folgenden zusätzlich die politische, wirtschaftliche und rechtliche Struktur sowie der IT-Reifegrad als qualitative Kriterien erörtert, wobei zusätzlich eine möglichst gleichmäßige Verteilung über die europäischen Regionen erzielt werden soll.

Politisch und rechtlich steht Deutschland sicherlich Österreich am nächsten. Vor allem besteht Österreich ebenso wie Deutschland aus starken Bundesländern, die über eigene Regierungen und Gesetzgebungskompetenzen verfügen. Außerdem weist Österreich eine ähnliche wirtschaftliche Struktur im Hinblick auf den Anteil mittelständischer Unternehmen auf, so dass sich die Einbeziehung in die engere Auswahl empfiehlt, obwohl Österreich in Bezug auf den Stand der Informationssicherheit nach statistischer Auswertung nicht unbedingt hervorsticht, sondern – auch in diesem Punkt – „lediglich" im Bereich Deutschlands liegt.

Außer Deutschland und Österreich besitzt unter den betrachteten Ländern nur noch Spanien den Bundesländern vergleichbare Gebietskörperschaften in Form der autonomen Gemeinschaften. Daher und aufgrund dessen, dass nach Möglichkeit auch ein südeuropäisches Land in die Analyse eingehen soll, wird Spanien zusammen mit Italien weitergehend betrachtet.

Die Eingrenzung der skandinavischen Länder stellte sich als schwierig heraus, da sowohl Schweden als auch Finnland und Dänemark in mehreren quantitativen Auswertungen vordere Plätze belegen. Da es beabsichtigt war, eine regionale Verteilung zu erhalten, sollten nicht alle skandinavischen Länder in den Vergleich einfließen. Die Wahl fiel aus mehreren Gründen auf Schweden. Zum einen aufgrund der hohen Zahl deutscher Unternehmensengagements in Schweden (Tochterfirmen, Beteiligungen, Filialen oder Repräsentanzen) mit etwa 870 Unternehmen, insgesamt rund 50.000 Beschäftigten und einem geschätzten Jahresumsatz von etwa 30 Milliarden. Dem gegenüber stehen 700 schwedische Engagements in Deutschland mit rund 140.000 Beschäftigten und einem Jahresumsatz von 45 Milliarden Euro[12]. Zudem stellt Schweden gemessen am BIP die größte skandinavische Volkswirtschaft dar und zeichnet sich durch hohe Forschungs- und Entwicklungsausgaben aus.

Die Daten zu den osteuropäischen Ländern, die ebenso vertreten sein sollen, geben ein uneinheitliches Bild. Die baltischen Staaten konnten sich vor allem im Hinblick auf den hohen Anteil mittelständischer Unternehmen empfehlen, stehen darüber hinaus aber auch in dem Ruf, in kurzer Zeit einen vergleichsweise hohen Grad der IT-Reife erreicht zu haben. So hat insbesondere Estland durch einen im April 2007 erfolgten Cyber-Angriff auf Regierungsportale, hinter dem ein anderer Staat vermutet wurde, zahlreiche Maßnahmen im Rahmen eines umfassenden 5-Jahres-Plans entworfen, um die Informationssicherheit zu verbessern (Ministry of Defence Estonia 2008).

Abschließend wurden die Niederlande in die Auswahl einbezogen. Die Daten zu den niederländischen Unternehmen weisen in einigen Auswertungen auf einen fortgeschrittenen Reifegrad bezüglich der Technologienutzung von Unternehmen und Gesellschaft sowie auf ein hohes Problembewusstsein hin.

Zusammengefasst ergibt sich also folgende Auswahl an Ländern für die weitere Betrachtung in dieser Studie: Estland, Großbritannien, Niederlande, Österreich, Schweden, Spanien. Daneben sind – wie eingangs – die USA als weiteres Land durch den Auftraggeber gesetzt gewesen.

[12]http://www.auswaertiges-amt.de/DE/Aussenpolitik/Laender/Laenderinfos/Finnland/Bilateral_node.html, 20.05.2014

4 Vergleichsanalyse zu Stand der Informationssicherheit

Insgesamt konnten 56 Initiativen entsprechend der oben beschriebenen Anforderungen recherchiert werden, wobei sich im Hinblick auf die Anzahl ein deutliches Übergewicht an deutschen Initiativen ergab. Der Grund dafür dürfte nicht zuletzt in der einleitend schon erwähnten Einrichtung der Task Force „IT-Sicherheit in der Wirtschaft“ im BMWi liegen, die mehr als die Hälfte der Initiativen auf den Weg brachte. Eine vergleichbare konzertierte und auf KMU fokussierte Anstrengung konnte so in keinem der anderen Länder beobachtet werden. Abbildung 16 gibt einen Überblick zur Aufteilung der Initiativen nach Ländern:

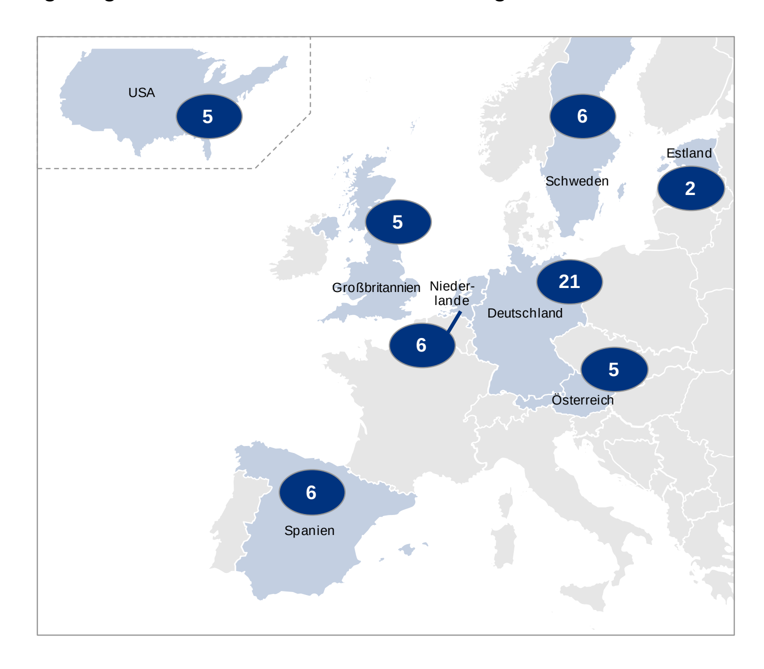


Abbildung 16: Anzahl betrachtete Initiativen aufgeteilt nach Ländern.

Bereits in den Vorarbeiten wurde offensichtlich, dass sich die 56 untersuchten Initiativen in Form, Ziel, Komplexität und Inhalt mitunter deutlich unterscheiden. Um aus diesen zahlreichen und heterogenen Informationen mögliche Gemeinsamkeiten, Zusammenhänge, Schwerpunkte und Trends zu ermitteln, bedurfte es einer systematischen Erfassung. Die dazu genutzten Kriterien sollten alle die für das Projektziel relevanten Informationen abbilden, ohne dabei jedoch die Übersichtlichkeit durch unwesentliche Details zu beeinträchtigen. Aus diesem Verständnis ergeben sich die folgenden vier Anforderungen an die Erfassung:

- Vollständigkeit: Zur Identifikation möglicher zukünftiger Maßnahmen des BMWi genügt es nicht, allein die technischen Details einer Initiative zu erfassen. Darüber hinaus müssen auch Umfeld und Intention der jeweiligen Initiative erfasst werden.
- Genauigkeit: Merkmale einzelner Initiativen müssen genau konkretisiert werden, um präzise Aussagen zu treffen. Eine Auskunft, dass die betrachtete Initiative das Ziel hat, die Sicherheit von KMU im Internet zu erhöhen, ist nur bedingt aussagekräftig. Allein aus informationstechnologischer Sicht gilt es, eine weitergehende Unterscheidung, beispielsweise nach IT-Netzen und IT-Anwendungen vorzunehmen. Darüber hinaus sind mögliche Maßnahmen oder eventuelle Defizite von Interesse.

- Konsistenz: Im Bereich der Informationstechnologie existieren bereits mehrere Standards, auf deren Basis Informationssicherheit im Unternehmen beurteilt, optimiert und zertifiziert wird. Zu diesen Normen gehören beispielsweise die BSI-Standards 101-104 oder die ISO-Reihe 27000. Des Weiteren haben in der Vergangenheit Studien Defizite in KMU und Instrumente zu deren Behebung untersucht. Dieses damit verbundene Wissen zu nutzen, ist aus Gründen der Arbeitseffizienz sinnvoll und für die Entwicklung von zukünftigen Initiativen geboten.
- Übersichtlichkeit: Es ist offensichtlich, dass diese Anforderung mit den beiden erstgenannten im Konflikt steht. So können beispielsweise die erwähnten Standards nicht ohne weiteres übernommen werden, da diese eher Anleitungen zur Vereinheitlichung denn Analyseinstrumente darstellen. Somit gilt es, bei der Formulierung der Kriterien die Balance zwischen technischer Genauigkeit und informationellen Mehrwert zu finden.

Ausgehend von diesen Anforderungen ergaben sich insgesamt 13 Kriterien mit einer Vielzahl von vorgegebenen möglichen Merkmalen, mittels der die Initiativen beschrieben werden konnten. Die Ergebnisse aus der Erfassung dieser 13 Kriterien lassen sich in vier Themenfelder zusammenfassen:

- Rahmen der Initiativen,
- Intentionen der untersuchten Initiativen,
- Ansätze und Mittel zur Verbesserung der Informationssicherheit,
- Wirkungen der Initiativen.

Die folgenden Kapitel sind somit auf der ersten Ebene nach diesen Themenfeldern und auf der zweiten Ebene nach den jeweils korrespondieren Kriterien gegliedert.

4.1 Rahmen der Initiativen

Der Vergleich von Initiativen erfordert im ersten Schritt die Erfassung der Rahmenbedingungen. Dazu gehören

- der politische Kontext, in dem die Initiative entstanden ist,
- die Akteure,
- die Adressaten und
- die Laufzeiten.

Obwohl die Initiativen infolge des Projektauftrags einen klaren Fokus auf Informationssicherheit in KMU haben, so weisen diese – wie im Folgenden erläutert wird – hinsichtlich dieser Kriterien doch zum Teil erhebliche Unterschiede mit Folgen für deren Übertragbarkeit in das wirtschaftliche Umfeld der Bundesrepublik Deutschland auf.

4.1.1 Politischer Kontext

Initiativen unter Beteiligung des Staates beziehungsweise der Repräsentanzen der öffentlichen Verwaltung stehen immer in einem politischen Kontext. Die Politik kann mit einer Initiative zur Informationssicherheit verschiedene Ziele verfolgen. Die tatsächliche Intention

muss dabei nicht immer unmittelbar erkennbar sein. Tatsächlich haben die Interviews insbesondere im Hinblick auf dieses Merkmal mitunter unerwartete Antworten geliefert.

Des Weiteren lassen sich die politischen Ziele einer Initiative nur selten separieren. Insofern geben die Erkenntnisse zu den nachstehend erläuterten Merkmalen in erster Linie einen Aufschluss darüber, "wessen Geistes Kind" eine Initiative ist. Die nachfolgende Abbildung gibt einen Überblick über das politische Umfeld ihrer Entstehung.

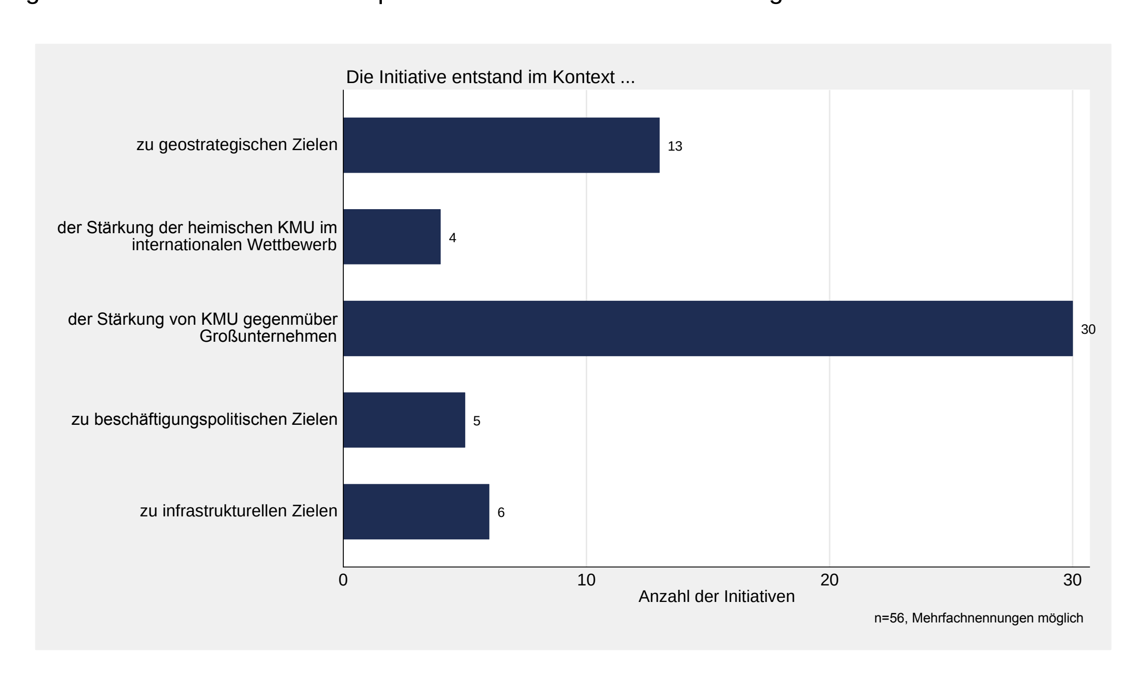


Abbildung 17: Politischer Kontext der Initiativen

Wie angesichts des Untersuchungsgegenstands zu erwarten war, entstanden die Initiativen in erster Linie aus der Absicht heraus, mittelständischen Unternehmen im Wettbewerb mit großen Konkurrenten den Rücken zu stärken. Dennoch verfolgt beziehungsweise verfolgte – etwas überraschend – ein erheblicher Teil der Initiativen im Ausgang geostrategische Ziele, wozu im weiteren Sinne auch infrastrukturelle Ziele gehören. Die Auswertung nach Ländern zeigt, wenn auch allein aufgrund der Fallzahlen nicht immer in allen Ländern alle Zellen belegt sein können, mehrere Auffälligkeiten.

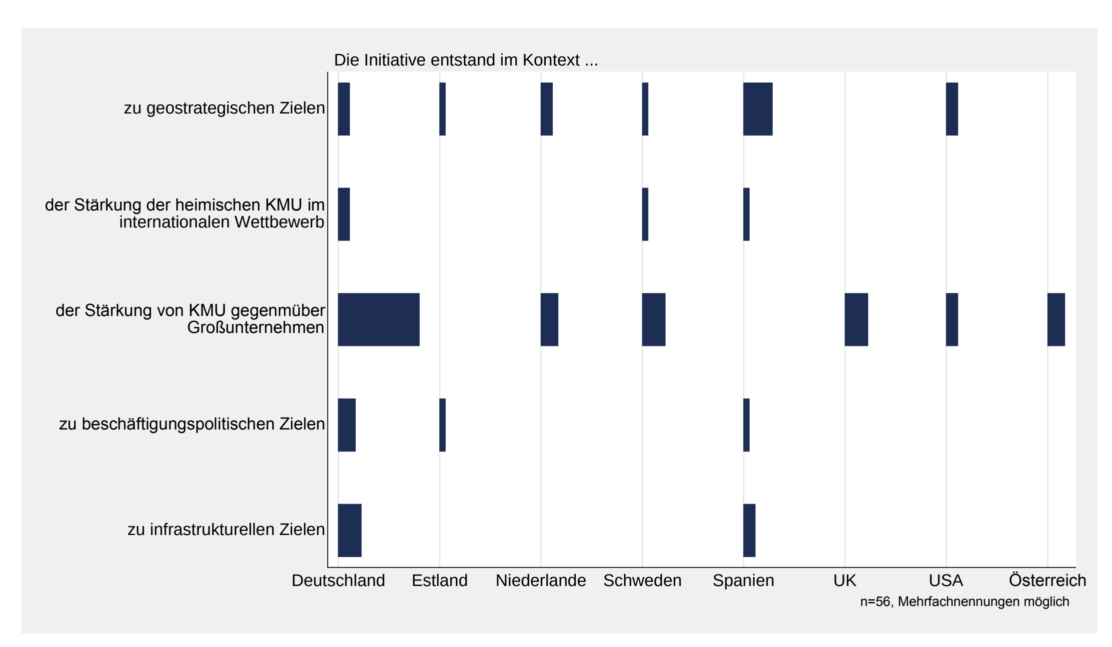


Abbildung 18: Politischer Kontext der Initiativen

Erstens haben Estland und Spanien auf den ersten Blick nicht die Absicht, gezielt KMU zu fördern. Während in Estland die Mittelstandsförderung tatsächlich keine nennenswerte Rolle spielt, stand in Spanien zwar zunächst der Schutz der Infrastruktur im Mittelpunkt, die Initiativen richteten beziehungsweise richten sich dann aber doch auch an KMU. Zweitens verfolgen Großbritannien und Österreich ausschließlich mittelstandspolitische Ziele. Vor allem für Großbritannien mag dies überraschen, da doch im Vorfeld der Untersuchung – vermutlich auch infolge der öffentlichen Diskussion – der Eindruck entstand, das Land würde in erster Linie geostrategische Interessen durchsetzen wollen. Der Grund für den ausgeprägten Mittelstandsbezug in beiden Ländern dürfte nicht zuletzt in dem Engagement der jeweiligen unternehmensnahen Einrichtungen liegen, wie an späterer Stelle noch zu zeigen ist. Im Folgenden werden nun die einzelnen Merkmale näher erläutert.

Geostrategische Ziele

Es mag auf den ersten Blick verwundern, wenn bei Initiativen zur virtuellen Welt von geostrategischen Belangen die Rede ist. Allerdings haben gerade die Vorkommnisse in der jüngsten Zeit gezeigt, dass das Internet durchaus zur Durchsetzung nationaler Interessen genutzt wird, selbst wenn eine solche Absicht etwa unter der Stärkung der heimischen Unternehmen im internationalen Wettbewerb kommuniziert wird. So stellt zum Beispiel die 2011 für Großbritannien verkündete Strategie Initiativen in Aussicht, die die „kommerzielle Ausbeutung“ der Expertise des britischen Nachrichtendienstes GCHQ ermöglichen sollen (OECD 2012, S. 29). Allerdings folgten dieser Ankündigung – wie die Interviews ergaben – keine konkreten Initiativen. Inwieweit die Vorkommnisse um den GCHQ hier eine Rolle spielen, lässt sich auch nach intensivem Nachfragen nicht feststellen. Zwar bieten Nachrichtendienste – wie in Deutschland der Wirtschaftsschutz beim Bundesamt für Verfassungsschutz – grundsätzlich ihre Unterstützung auch für KMU an, Initiativen in der Abgrenzung dieses Projektes konnten jedoch in keinem der untersuchten Länder beobachtet werden.

Eine Initiative kann aber natürlich auch den Zweck verfolgen, sich vor den geostrategischen Interessen anderer Länder zu schützen. So ist die erste *Cyber Security Strategy* Estlands

2008 unter dem Eindruck der Attacken im Jahr zuvor entstanden (Minister of Economic Affairs and Communications 2012). Eine aus dieser Strategie resultierende Initiative, die KMU zumindest im weiteren Sinne betrifft, ist die Bereitstellung des *Estonian Security Interoperability Framewor*k, der Unternehmen den sicheren Datenaustausch mit staatlichen IT-Systemen ermöglichen soll.

Zu den weiteren gefundenen Initiativen, die vor allzu viel Neugier ausländischer Organisationen schützen sollen, gehören zum einen die verschiedenen Warndienste respektive CERTs sowie die Bemühungen um den Schutz der heimischen (kritischen) Infrastruktur durch Penetrationstests. Zum anderen entstanden nach Auskunft der Interviewpartner einige Initiativen im Kontext der Verteidigung nationaler Interessen, die auf den ersten Blick nur wenig mit geostrategischen Zielen assoziiert werden dürften. Dabei handelt es sich um Schulungen und Informationsmaterialien in Spanien und den USA sowie um Bewusstseinsinitiativen in Spanien und den Niederlanden. Im Vergleich mit anderen mittelstandsbezogenen Maßnahmen sind diese Initiativen nur wenig spezifisch. Anders ausgedrückt, die Initiativen haben KMU als nationale Sicherheitslücken ausgemacht, die durch Bewusstseinsförderung und Hilfen zu schließen sind.

Wettbewerbspolitische Ziele

Initiativen zur Informationssicherheit können dazu genutzt werden, dem heimischen Mittelstand international Wettbewerbsvorteile zu verschaffen. Dabei steht die IT-Sicherheit der eigenen KMU zwar nicht im Vordergrund, indirekt jedoch – so die Argumentation – profitieren auch die heimischen Mittelständler von der gestiegenen Wettbewerbsfähigkeit der eigenen IT-Sicherheitsbranche. Dieses Ziel verfolgen nach Einschätzung der ENISA beziehungsweise der OECD beispielsweise Initiativen in Großbritannien und den USA[13]. Allerdings konnten solche Initiativen, die tatsächlich die Informationssicherheit in KMU verbessern, in den betreffenden Ländern nicht identifiziert werden. Gefunden wurden lediglich zwei Initiativen aus Deutschland – *SimoBIT* und *IT Security Made in Germany* – und mit *Voice of the Industry* eine Initiative aus Spanien, die zumindest im Ansatz diese Idee verfolgen.

Das im Zusammenhang mit diesem Projekt weitaus bedeutendere wettbewerbspolitische Ziel entstammt der klassischen Mittelstandsförderung, die die größenbedingten Nachteile von KMU zu mildern sucht. Die dazu genutzten Initiativen lassen sich – fast vollständig – gliedern in Informationsangebote, Schulungen, Beratungsleistungen und Kampagnen. Das in der Mittelstandsförderung ansonsten häufiger genutzte Instrument in Form von Zuschüssen und vergünstigten Darlehen bleibt hingegen nahezu unbeachtet. Die Initiativen scheinen größtenteils bislang vor allem den Bedarf nach einer Förderung bei KMU überhaupt erst zu wecken.

Beschäftigungspolitische Ziele

Initiativen, die letztlich einen Beitrag zur Informationssicherheit in KMU leisten, können durchaus aus der Absicht entstanden sein, Arbeitsplätze zu sichern oder zu schaffen. Sofern allerdings solche Initiativen außerhalb Deutschlands existieren, konnte kein direkter Bezug

[13] Vgl. zu Großbritannien ENISA (2012) sowie zu den USA OECD (2012).

zur Informationssicherheit festgestellt werden. Zwar werden auch in anderen Ländern Erwerbspersonen im Hinblick auf Fragen zur Informationssicherheit weitergebildet, jedoch erfolgt dies in der Regel unabhängig von mittelständischen Unternehmen. Somit bleiben die deutschen Initiativen *SimoBIT*, *Trusted Cloud* und *nrw.units*, die einerseits eine Form von Wirtschaftsförderung sind, andererseits aber auch Rückwirkungen auf die Informationssicherheit deutscher KMU haben, an dieser Stelle ohne einen Vergleich.

Infrastrukturelle Ziele

Die digitale Grundversorgung wird durch den Ausbau sowie durch den Schutz des Zugangs zum Netz gewährleistet. So ist es denn auch ein Ziel der IKT-Strategie der Bundesregierung, durch eine Reihe von Maßnahmen die digitale Grundversorgung sicherzustellen.

Prinzipiell richten sich Initiativen mit dem Fokus auf die Infrastruktur an große Unternehmen in Form von Netzbetreibern oder anderen kritischen Versorgungsunternehmen. Dennoch können auch KMU einen Beitrag zum Schutz der Infrastruktur leisten, wie in Deutschland das Beispiel der *Initiative-S* zeigt, die sich insbesondere an KMU richtet. Allerdings blieb die Recherche in anderen Ländern weitgehend ohne Erfolg. Lediglich die bereits im Zusammenhang mit den geostrategischen Zielen erläuterten wenig spezifischen Initiativen in Spanien entstanden unter anderem auch in der Absicht, die heimliche kritische Infrastruktur schützen.

4.1.2 Akteure

Die Komplexität der Aufgabe, die Informationen eines Unternehmens zu schützen, spiegelt sich in dem breiten Spektrum der Akteure wider. Die ENISA gibt für Estland 26 auf dem Feld der Informationssicherheit aktive Einrichtungen an ENISA (2011a). Deutschland weist – zumindest im europäischen Vergleich unter den ausgesuchten Ländern – die meisten Einrichtungen mit insgesamt 71 Bundesbehörden, CERTs, Wirtschaftsverbänden und akademischen Einrichtungen sowie weiteren Organisationen auf (ENISA 2011b). Da die Länderberichte der ENISA keine regionalen oder lokalen Gebietskörperschaften betrachten, dürfte die tatsächliche Zahl insbesondere in Deutschland noch weitaus höher liegen.

Um die Initiativen möglichst genau zu erfassen und Unterschiede in den Ländern aufdecken zu können, wurden die Akteure in Kategorien gegliedert, deren Verteilung die nachstehende Abbildung wiedergibt.

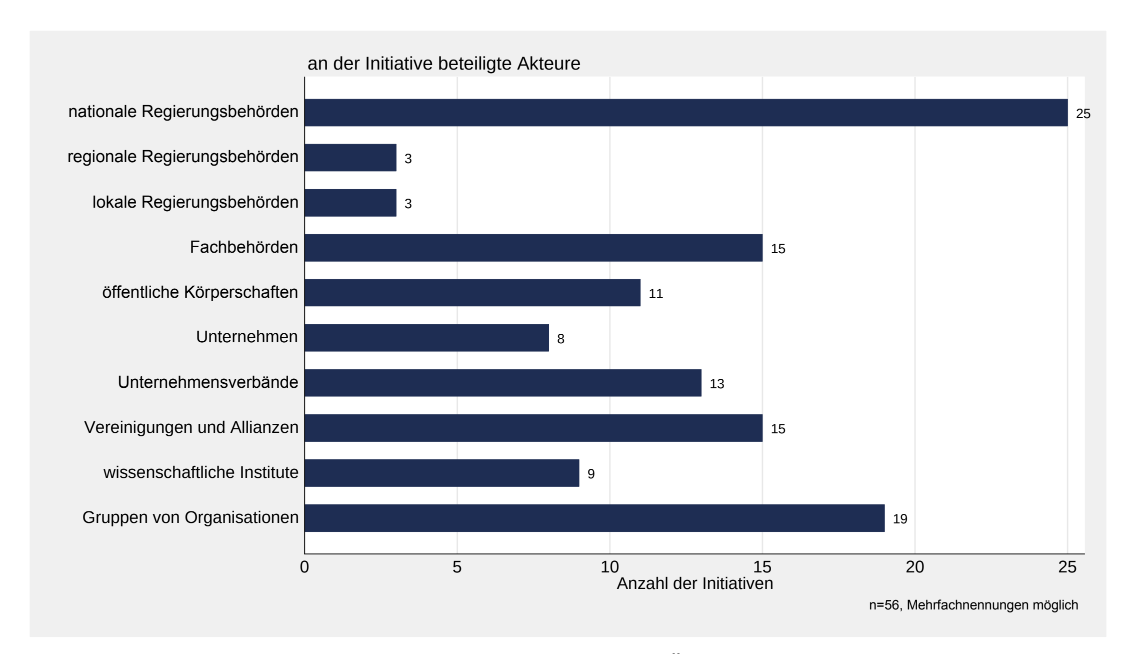


Abbildung 19:Die Akteure im Überblick

Die Dominanz staatlicher Einrichtungen und insbesondere nationaler Regierungsbehörden scheint angesichts des Untersuchungsgegenstands nicht erstaunlich zu sein. Die Betrachtung der einzelnen Länder allerdings zeigt ein differenzierteres Bild, bei dem sich die jeweils treibenden Kräfte doch unterscheiden.

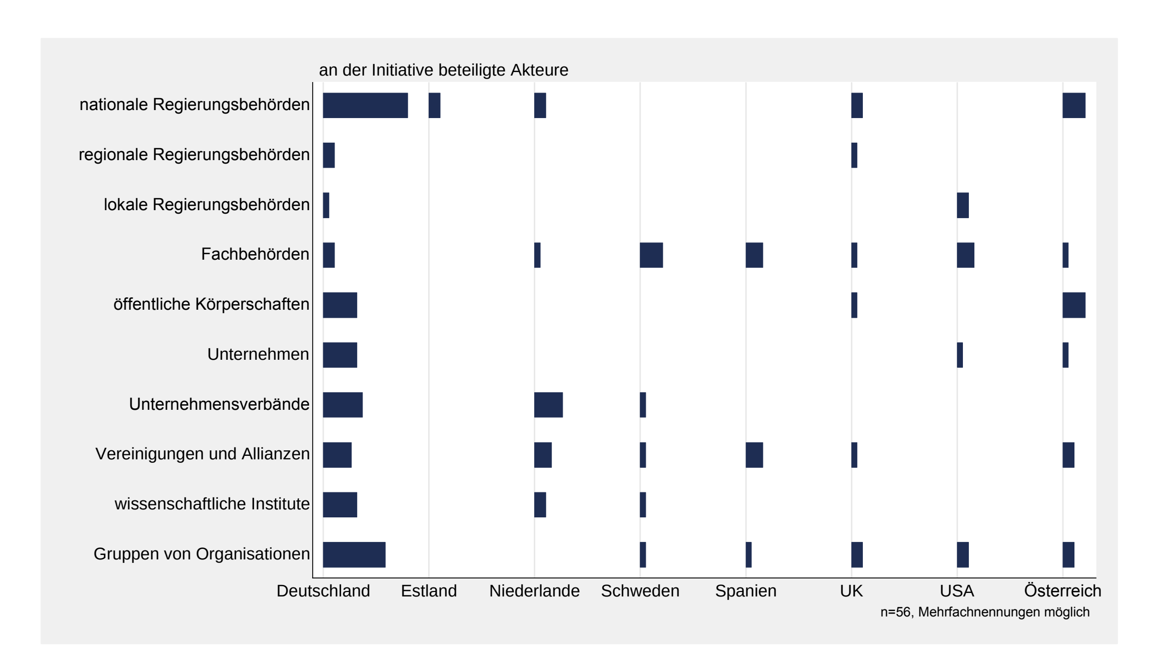


Abbildung 20: Die Akteure in den einzelnen Ländern

Nationale Regierungsbehörden besitzen vor allem in Deutschland eine herausragende Rolle. Ähnlich wichtig, wenn auch nicht ganz so dominant, sind die österreichischen Ministerien sowie das Kanzleramt und das britische *Department for Business Innovation and Skills* für die Bemühungen um mehr Informationssicherheit in KMU. Dieser Gruppe scheint nach

Abbildung 20 auch Estland anzugehören, das allerdings in diesem Grund eine Sonderrolle einnimmt, auf die im nachstehenden Abschnitt noch eingegangen wird.

Die geringe Anzahl von Initiativen, bei denen sich regionale oder lokale Regierungsbehörden als treibende Kraft gezeigt haben, legt nahe, dass Informationssicherheit doch in erster Linie selbst in föderalen Systemen als nationale Aufgabe gesehen wird.

Weiterhin fällt auf, dass in den Ländern, in denen nationale Regierungsbehörden nicht als aktive Akteure nach außen erscheinen, die jeweils zuständigen Fachbehörden eine hervorgehobene Bedeutung besitzen. Der Grund dafür liegt sicherlich weniger im Desinteresse der jeweils zuständigen Ministerien, sondern dürfte vielmehr aus der Verlagerung von Kompetenzen auf die nachgeordnete Ebene resultieren.

Die letzten in der Abbildung dargestellten staatlichen Einrichtungen sind die öffentlichen Körperschaften oder genauer die jeweiligen Kammern. Zwar handelt es sich bei den britischen *Chambers of Commerce* nicht tatsächlich um Behörden, der besseren Vergleichbarkeit wegen wurden diese hier auch den öffentlichen Körperschaften zugeordnet. Die starke Stellung der Kammern vor allem in Deutschland und Österreich mag zumindest zum Teil auch die im vorangegangenen Kapitel angesprochene Bedeutung der Mittelstandsförderung in diesen Ländern erklären.

Die Gliederung der verbleibenden Organisationen illustriert zum einen, dass viele Initiativen durch den Zusammenschluss einer Reihe von Unternehmen und anderen privaten sowie öffentlichen Einrichtungen getragen werden. Zum anderen fällt auf, dass einzelne Unternehmen allein nur selten als treibende Kraft erscheinen.

Die folgenden Ausführungen gehen auf die Rolle der einzelnen Akteure sowie auf besonders interessante Akteure ein.

Staatliche Einrichtungen

Unter staatlichen Einrichtungen werden hier allgemein Behörden im Sinne des § 1 VwVfG (Verwaltungsverfahrensgesetz) verstanden. In Anbetracht der Intention des Projekts sollte der Fokus sicherlich auf den Stellen liegen, die entweder dem BMWi vergleichbar sind oder in einem engen respektive nachgeordneten Verhältnis zu diesem stehen. Tatsächlich ist das BMWi in Deutschland der maßgebliche Treiber im Hinblick auf die Informationssicherheit in KMU. Das BMWi ist an 18 der 21 in Deutschland einbezogenen Initiativen maßgeblich beteiligt. International jedoch lässt sich eine solch starke Stellung des Wirtschaftsressorts nicht feststellen. Lediglich bei vier Initiativen ist ein Ministerium aus dem Ressort Wirtschaft ein wichtiger Akteur, fünf Ministerien hingegen sind den Ressorts Inneres, Justiz oder Verteidigung zuzurechnen. Dieses Verhältnis ändert sich auch dann nicht substanziell, wenn die nachgeordneten nationalen Fachbehörden sowie Körperschaften in die Rechnung einbezogen werden. So sind außerhalb Deutschlands die Ressorts Wirtschaft einerseits und Inneres und Justiz andererseits in etwa zu gleichen Teilen an den Bemühungen um mehr Informationssicherheit in KMU beteiligt. Das Verteidigungsressort hingegen ist mit der *Swedish Civil Contingencies Agency* (MSB) nur in zwei Initiativen von tragender Bedeutung.

Die Frage, inwieweit die Zugehörigkeit einer staatlichen Einrichtung zu einem Ressort einen Einfluss auf die Initiative besitzt, lässt sich nicht mit einem einfachen Ja oder Nein beantworten. Über alle Initiativen hinweg ist tatsächlich eine Tendenz dahingehend zu beobachten,

dass Behörden aus dem Bereich Wirtschaft eher Ziele der Mittelstandsförderung und Behörden aus den Bereichen Inneres und Justiz eher geostrategische beziehungsweise infrastrukturelle Ziele verfolgen. Allerdings ist dieser Zusammenhang keineswegs zwingend. Zur Erklärung bieten sich zwei Gründe an: Erstens werden viele Initiativen von mehreren Einrichtungen getragen. So spielen zum Beispiel bei der Initiative *E-Crime Wales* die walisischen Polizeibehörden eine herausragende Rolle. Gleichzeitig ist aber auch die *Federation of Small Businesses* an der Initiative beteiligt, so dass letztlich doch die Förderung der KMU im Vordergrund steht. Ähnlich ist die Polizei Österreich zusammen mit der *Wirtschaftskammer Österreich* in die Roadshow *Schutz vor Cyberkriminalität* eingebunden. Zweitens hat die gesellschaftspolitische Ausrichtung eines Landes mitunter einen größeren Einfluss als die Ressortzugehörigkeit. Ein gutes Beispiel zur Illustration ist Estland, das unter dem Eindruck der Attacke von 2007 die Sicherheit der nationalen Einrichtungen und Infrastruktur in den Mittelpunkt seiner Politik rückte. Konsequenterweise lag dann die Zuständigkeit für den Aufbau einer Behörde zur Informationssicherheit zunächst beim Verteidigungsministerium und wurde erst danach auf das Wirtschaftsministerium übertragen. So verwundert es nicht, dass alle Bemühungen Estlands – auch unter Beteiligung des Wirtschaftsministeriums – in erster Linie der nationalen Sicherheit dienen. Umgekehrt findet sich mit dem *Business Crime Reduction Centre* eine Initiative in der Auswahl, die ohne Beteiligung einer wirtschaftsnahen Organisation speziell ausgebildete Polizeibeamte aus der Region *Yorkshire and the Humber* als kostenlose Berater Unternehmen zur Verfügung stellt.

Im Hinblick auf die von den staatlichen Einrichtungen wahrgenommenen Rollen lässt sich für Deutschland feststellen, dass der Staat 17 von 21 einbezogenen Initiativen finanziert, wobei das BMWi allein die Mittel für 15 Initiativen aufbringt. Für 10 Initiativen stellen Behörden Ressourcen – in der Regel Personal – zur Verfügung und bei 8 unterstützen Behörden die Initiativen auf andere Weise – zum Beispiel als Multiplikatoren oder durch die Bereitstellung von Räumen. Ein Vergleich mit den anderen einzelnen Ländern verbietet sich aufgrund der geringen Fallzahlen zwar, über alle Länder hinweg jedoch ist ersichtlich, dass außerhalb Deutschlands staatliche Einrichtungen Initiativen vorzugsweise mit Ressourcen oder in ähnlicher Weise beteiligen. Nur 10 der betrachteten Initiativen werden durch staatliche Stellen finanziert, 12 hingegen durch Ressourcen und 8 Initiativen auf andere Weise unterstützt. Von allen untersuchten Ländern weist Großbritannien mit den Rollen, die das *Department for Business Innovation and Skills* (BIS) sowie die *Chambers of Commerce* spielen, noch die größte Ähnlichkeit zu Deutschland auf, wobei diese Einschätzung bei lediglich 5 Initiativen mehr qualitativ denn quantitativ sein kann.

Unternehmen und Institute

Einzelne Unternehmen oder Institute sind für eine Initiative nur selten von maßgeblicher Bedeutung. Der Kreis wird sogar nochmals kleiner, wenn nur noch diejenigen betrachtet werden, die nicht als Auftraggeber, sondern aus eigenem Antrieb, also ohne finanzielle Gegenleistung eine Initiative tragen. So stellt beispielsweise die *Datev eG* nicht nur den größten Teil der Ressourcen, sondern auch das Hosting für den DsiN-Sicherheitscheck zur Verfügung. Ähnlich hat Microsoft Österreich die Plattform *Sicher im Internet* ins Leben gerufen und betreibt diese auch mit ideeller Unterstützung des österreichischen Bundesinnenministeriums. Eine etwas andere Konstruktion hat das slowakische IT-Sicherheitsunternehmen *ESET* in den USA gewählt. Neben der vom Unternehmen finanzierten Stiftung *Securing Our e*City unterstützen *Donors and Partners* die kostenlos angebotenen Schulungen sowohl finanziell als auch in anderer Form.

Die Beteiligung von Instituten konnte außerhalb Deutschlands nur in zwei Fällen festgestellt werden. Eine Begleitforschung, wie sie in einigen der vom BMWi finanzierten Initiativen durchgeführt wird, ist dabei nicht vorgesehen. In Schweden bietet die *Königlich Technische Hochschule Stockholm* – gegen eine individuell zu verhandelnde Gebühr – eintägige Seminare für KMU an und in den Niederlanden stellt die *Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek* – Niederländische Organisation für Angewandte Naturwissenschaftliche Forschung, in etwa vergleichbar mit der Fraunhofer-Gesellschaft, kurz TNO – KMU Wissen aus der eigenen Forschung zur Verfügung.

Verbände, Vereinigungen und Allianzen

Einzelne Unternehmen und Institute treten zwar nur selten als maßgeblich treibende Kraft einer Initiative in Erscheinung, umso häufiger jedoch sind diese in Unternehmens- oder Interessenverbänden, anderen Vereinigungen mit eigener Rechtspersönlichkeit und losen Gruppen respektive Allianzen vertreten. Solche Zusammenschlüsse sind – mit Ausnahme Estlands – in allen Ländern an insgesamt 34 der 56 einbezogenen Initiativen beteiligt.

Ein Vergleich nach Ländern ist, wie schon im Abschnitt zu den staatlichen Einrichtungen, aufgrund der im Vergleich zu Deutschland wenigen Initiativen schwierig. Für Deutschland besitzen Verbände, Vereinigungen und Allianzen auf jeden Fall eine große Bedeutung. In 15 der 21 Initiativen sind diese beteiligt oder sogar hauptsächlich verantwortlich. Aber auch in den anderen Ländern spielen solche Organisationen und Gruppen eine wichtige Rolle. Immerhin 19 der verbleibenden 35 Initiativen sind so entstanden.

Die Organisationen und Gruppen stellen den Initiativen vor allem personelle und technische Ressourcen zur Verfügung oder unterstützen diese als Multiplikatoren. Darüber hinaus unterstützen einige der Organisationen sowie einzelne Mitglieder aus den betreffenden Gruppen einen Teil der Initiativen mit finanziellen Mitteln.

Zu den Verbänden gehören sowohl allgemeine Unternehmensverbände wie auch spezialisierte IT-Branchenverbände. Die Mitglieder der anderen Vereinigungen und Allianzen decken oftmals ein breites Spektrum an Organisationen ab. Neben Softwareunternehmen, Beratungsgesellschaften und Wirtschaftsverbänden finden sich Forschungsinstitute ebenso wie Polizeibehörden und Regierungseinrichtungen. Auf diese Weise kooperieren staatliche Einrichtungen nicht nur mit solchen Gruppen, sondern sind mitunter auch selbst Teil derselben. So sind beispielsweise das BMWi und das *Bundesministerium des Innern* (BMI) im Beirat des *Deutschland sicher im Netz e.V.*, das österreichische *Bundesministerium für Finanzen* als Mitglied im *A-SIT Zentrum für sichere Informationstechnologie - Austria* oder das niederländische Wirtschaftsministerium in dem Zusammenschluss *Digibewust* vertreten.

4.1.3 Adressaten

Das Projekt adressiert, wie in Kapitel 2.1 erläutert, mittelständische Unternehmen. Dementsprechend interessieren hier auch nur Initiativen, die einen expliziten Bezug zu KMU aufweisen. Diese Einschränkung scheint auch insbesondere deshalb ratsam, weil die Ergebnisse der Untersuchung zu Hinweisen über zukünftige Initiativen im Bereich des BMWi führen sollen. Dennoch darf die Erfassung nicht zu restriktiv vorgehen, um gegebenenfalls interessante Initiativen nicht auszuschließen, wenn diese ein breiteres Spektrum an

Adressaten haben. Tatsächlich richten sich die recherchierten Initiativen in unterschiedlichem Maße an KMU, wie die nachstehende Abbildung illustriert:

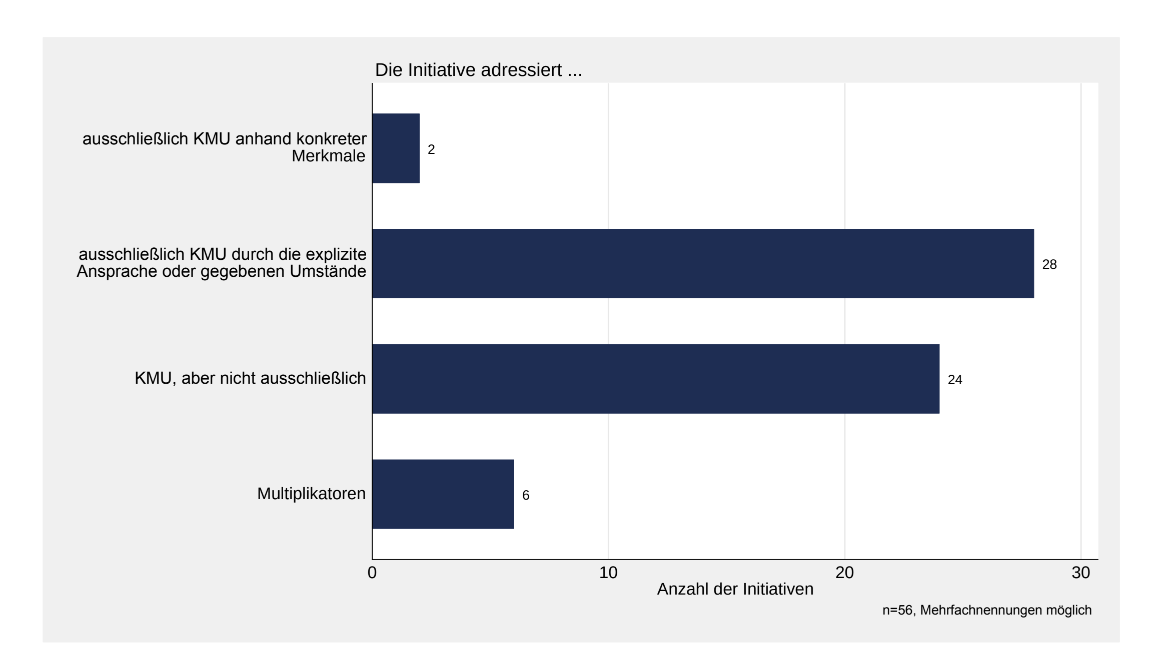


Abbildung 21: Die Adressaten im Überblick

Die meisten Initiativen lassen sich in zwei Gruppen einteilen. Beiden ist gemeinsam, dass sie bei der Inanspruchnahme des jeweiligen Angebots keine Restriktionen im Hinblick auf die Unternehmensgröße setzen. Grundsätzlich könnten die Angebote von allen Unternehmen genutzt werden. Dennoch richten sich einige Angebote indirekt doch ausschließlich an KMU. Erstens adressieren Initiativen mitunter Wirtschaftsbereiche, in denen aufgrund der erbrachten Leistungen nur KMU arbeiten. Solche Angebote konnten allerdings nur in Deutschland festgestellt werden. Dabei handelt es sich um die Initiativen „IT-Sicherheit im Handwerk“ und das *komzet@hwk*, die beide ausschließlich Handwerksunternehmen ansprechen. Zweitens sind manche Angebote derart spezifisch, das größere Unternehmen schlicht kein Interesse daran haben. So stellen zum Beispiel die Initiativen *ISA+* in Deutschland und der *Small Biz Cyber Planner* in den USA Richtlinien zur Sicherstellung der Informationssicherheit zur Verfügung, die für große Unternehmen nicht geeignet wären.

Darüber hinaus wurde eine Reihe von Initiativen identifiziert, die KMU zwar explizit ansprechen, deren Angebote aber durchaus auch von größeren Unternehmen genutzt werden können. Hierzu gehören die diversen Informationsplattformen zur Informationssicherheit, deren Beiträge nicht nur für KMU von Interesse sein müssen (zum Beispiel *E-Crime Wales* und *Get Safe Online* in Großbritannien, *Deutschland sicher im Netz*, *it-safe.at* in Österreich, *Stop Cybercrime* sowie *Bescherm je bedrijf* in den Niederlanden oder das schwedische Informationsportal). Aber auch Schulungs- und Beratungsangebote, die sich eigentlich an KMU richten, finden durchaus das Interesse von Großunternehmen. So musste eine Initiative, die kostenlose Online-Seminare für KMU anbot, feststellen, dass rund ein Viertel der Teilnehmer in größeren Unternehmen beschäftigt ist. Nach Einschätzung des Trägers wollten diese Unternehmen so ihren eigenen Stand überprüfen.

Initiativen, deren Leistungen Unternehmen nur dann in Anspruch nehmen konnten beziehungsweise können, wenn sie tatsächlich die Merkmale eines KMU aufweisen, konnten nur

in zwei Fällen identifiziert werden. Im ersten Fall handelt es sich um die Teilnahme an einem Wettbewerb mit Vergabe eines Preises, im zweiten um Gutscheine für eine Beratung durch einen IT-Sicherheitsexperten.

Neben all diesen Initiativen, die mehr oder weniger auf KMU fokussieren, existiert eine Vielzahl an Angeboten, die von vornherein KMU nur als Teilgruppe adressieren. Obwohl dabei auf den ersten Blick nicht immer ersichtlich ist, inwieweit die Initiative mittelständische Unternehmen explizit anspricht, kommen diese Initiativen dann doch oftmals in erster Linie mittelständischen Unternehmen zugute, wie die Auswertung der Beschäftigtengrößenklassen des *DsiN-Sicherheitschecks* zeigt (Brandl und Scharioth 2013). Solche Initiativen finden sich in allen untersuchten Ländern, wobei Lacey und James (2010) für Großbritannien zu dem Schluss kommen, dass dieser Ansatz oftmals nicht die Bedürfnisse von KMU trifft. Tatsächlich bieten einige der recherchierten Initiativen nur sehr allgemeine Informationen, die keinen wirklichen Nutzen zu haben scheinen. Allerdings sind in dieser Gruppe auch sehr konkrete Angebote enthalten, so dass die Exklusivität eines Angebots für KMU allein kein Kriterium für dessen Nutzen ist.

Die letzte Gruppe in Abbildung 21 stellt einen interessanten Ansatz dar, insbesondere um dem Problem geringer Reichweiten von Initiativen zur Informationssicherheit mit Hilfe von Multiplikatoren entgegenzuwirken. Solche Multiplikatoren können besonders vertrauenswürdige Personen in Form von Angehörigen der Freien Berufe und/oder fachkundige Dienstleister sein, die auf ihre Aufgaben durch die Initiative vorbereitet werden. Allerdings fand sich – mit einer Ausnahme in den Niederlanden, wobei es sich jedoch nur um einen einmaligen Kongress mit Verbandsvertretern handelt – außerhalb Deutschlands keine vergleichbare Initiative, wie Abbildung 22 zeigt:

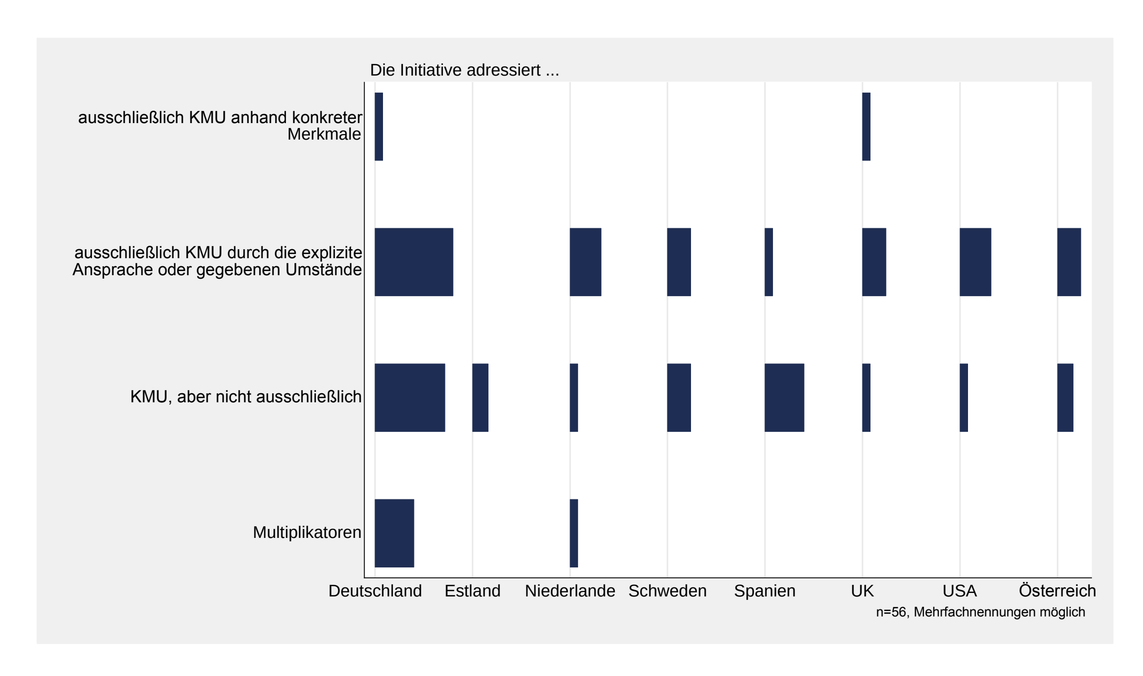


Abbildung 22: Die Adressaten nach Ländern

Die Abbildung zeigt weiterhin, dass in den Ländern, in denen die Initiativen eher im Kontext zu geostrategischen oder infrastrukturellen Zielen entstanden sind, die Angebote tendenziell Unternehmen allgemein adressieren, selbst wenn sich bei den geringen Fallzahlen die Berechnung einer Korrelation verbietet.

Schließlich wurden die Initiativen – wie schon oben im Hinblick auf die Handwerksunternehmen erwähnt – dahingehend gegliedert, inwieweit diese bestimmte Gruppen von KMU ansprechen. Diese Auswertung hat jedoch ebenfalls ergeben, dass solch gezielte Angebote nur in Deutschland beobachtet werden konnten.

4.1.4 Laufzeit

Zum Umfeld einer Initiative gehört abschließend, welchen Zeitraum die Sponsoren den Beteiligten einräumen. Bereits im Rahmen der Vorarbeiten zur Erfassung wurde ersichtlich, dass wohl einige Initiativen auf Dauer angelegt sind oder zumindest keiner Befristung unterliegen. Dennoch überraschte der hohe Anteil solcher Initiativen nach der Auswertung. Immerhin für die Hälfte der Angebote ist kein Ende in Sicht, wie Abbildung 23 zeigt:

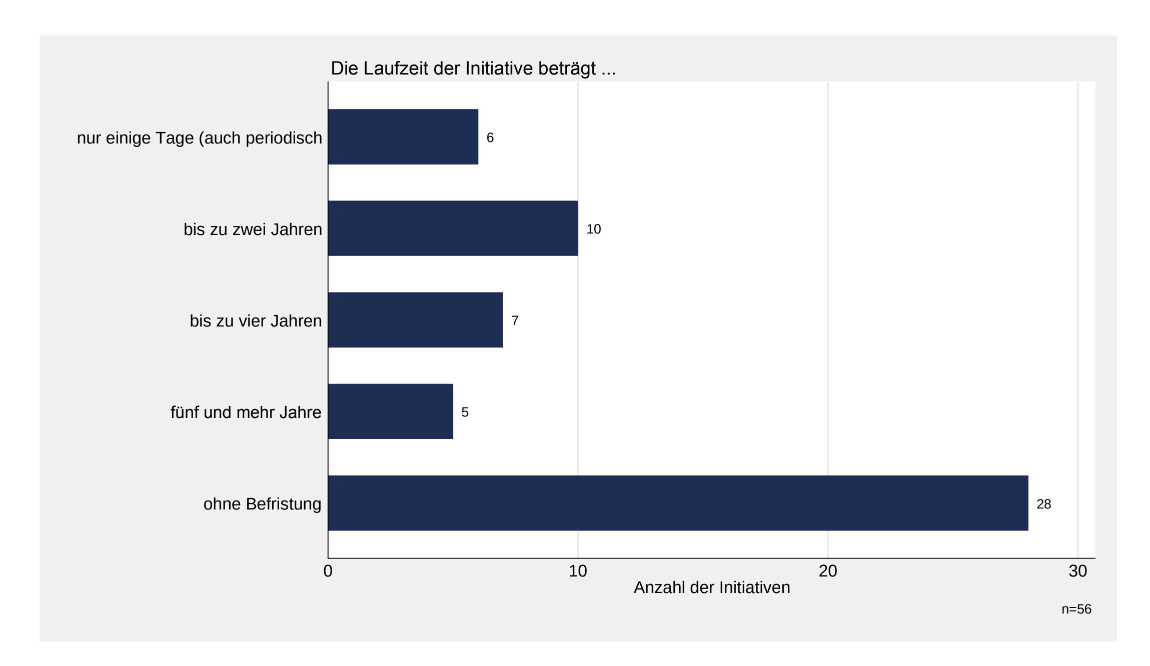


Abbildung 23: Die Laufzeiten der Initiativen im Überblick

Dabei handelt es sich nicht nur um laufend aktualisierte Informationsportale, sondern ebenso um Schulungsangebote und CERTs sowie im Falle des britischen *Business Crime Reduction Center* um ein dauerhaftes Beratungsangebot. Allerdings steigt die Wahrscheinlichkeit einer Befristung – selbst wenn, wie schon in den vorangegangenen Kapiteln, die Berechnung einer statistischen Signifikanz nicht ratsam ist – in den Fällen, in denen eine Behörde die Initiative finanziell unterstützt.

Die Auswertung nach Ländern zeigt, wie auch schon bei den Themen zuvor, mehrere Unterschiede, wobei diese allerdings nicht überinterpretiert werden sollten.

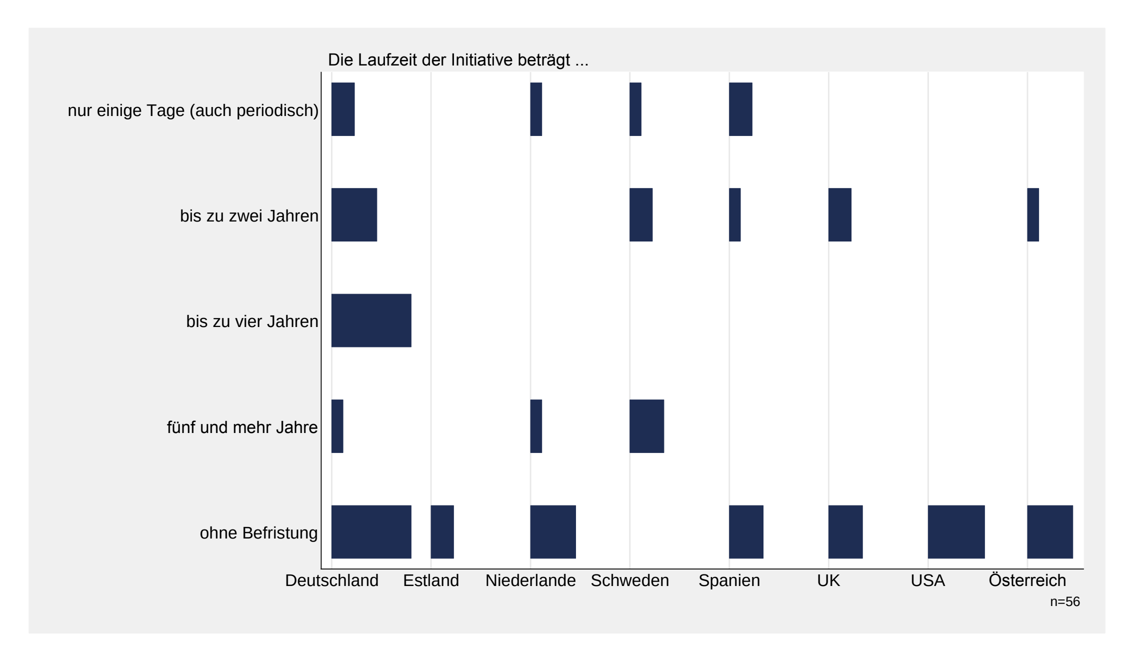


Abbildung 24: Die Laufzeiten der Initiativen nach Ländern

Unbefristete Initiativen sind in allen Ländern zu finden und dominieren in den USA sowie den Niederlanden sogar das Bild. Die Lücke bei Schweden resultiert daraus, dass das „Infoportal“ in seiner bisherigen Form nicht mehr durch die *Post and Telecom Authority*, sondern zukünftig von der *Swedish Civil Contingencies Agency* betreut wird. Prinzipiell besitzt aber auch diese Initiative kein festes Ende. Die deutlichste Auffälligkeit im Vergleich mit den anderen Ländern ist die hohe Zahl an Initiativen mit einem festen Zeitfenster von bis zu vier Jahren in Deutschland.

Weiterhin ist interessant, dass fünf von sechs der in Bezug auf den Zeitrahmen vergleichbaren Initiativen außerhalb Deutschlands im Kontext der klassischen Mittelstandspolitik entstanden sind. Hierzu gehören die britischen *Innovation Vouchers for Cyber Security* und die österreichischen *Schecks für Sicherheitschecks* sowie Schulungsangebote in Schweden (*ISIS*) und Großbritannien (*Bob's Business*), wobei für das derzeit noch laufende schwedische Angebot keine weitere Planung besteht und sich das britische E-Learning-Angebot mittlerweile ohne staatliche Unterstützung trägt.

4.1.5 Zusammenfassung

Vor dem Hintergrund der Frage nach einer möglichen Vergleichbarkeit der deutschen Bemühungen um eine bessere Informationssicherheit in KMU deutet die Betrachtung des jeweiligen Umfelds darauf hin, dass sich die untersuchten Länder weniger in feste Blöcke einteilen lassen als mehr graduell unterscheiden. Die geringste Ähnlichkeit zu Deutschland weist mit Sicherheit Estland auf. Die Politik konzentriert sich hier vollständig auf die Abwehr nationaler Gefahren. Eine Mittelstandspolitik zur gezielten Förderung von KMU ist zumindest auf dem Feld der Informationssicherheit nicht vorhanden. Selbst die prinzipiell vorhandenen Angebote schließen KMU von der unmittelbaren Nutzung aus: “As CERT Estonia does not provide services to end users, the latter should, in case of security incidents, turn to system administrators either at their Internet service provider or in their organisation, to network administrators or customer support” (Quelle: https://www.ria.ee/cert-estonia, 2. Mai 2014).

Bereits etwas schwieriger einzuordnen sind Spanien und Schweden. Hier verschwimmen zum Teil geostrategische Interessen und Mittelstandsförderung. In Spanien standen nach Auskunft der Interviewpartner eindeutig der Schutz der Infrastruktur beziehungsweise geostrategische Ziele Im Vordergrund. Dennoch bemühen sich die Initiativen um eine Einbeziehung mittelständischer Unternehmen, ohne dass jedoch ein mittelstandspolitischer Schwerpunkt zu erkennen wäre. So besteht zwar die Absicht, die bei großen spanischen Unternehmen durchgeführten Penetrationstests auf KMU zu übertragen, konkrete Vorstellungen fehlen aber noch. In Schweden dienen die Initiativen nach Auskunft der Interviewpartner zwar mehr der Mittelstandsförderung, bei genauerem Hinsehen zeigt sich jedoch, dass auch hier geostrategische Interessen eine größere Bedeutung haben. Die beiden Initiativen, die tatsächlich KMU adressieren, sind entweder wegen Erfolglosigkeit eingestellt worden oder erst noch in der Planungsphase. Zudem verschiebt sich infolge der Übernahme des „Infoportals" durch die *Swedish Civil Contingencies Agency* von der *Post and Telecom Authority* die Zuständigkeit vom Wirtschafts- zum Verteidigungsressort.

Im Hinblick auf das Potenzial, Initiativen zum Schutz geostrategischer Interessen oder der Infrastruktur ebenso zur Mittelstandsförderung zu nutzen, bleibt insgesamt festzustellen, dass Deutschland mit der *Initiative-S* hier bereits einen Schritt weiter ist. Der Grund dafür liegt vermutlich darin, dass mit der Initiative zwar die Nutzung des Internets in Deutschland gesichert werden soll, das Angebot aber aus der Perspektive der Mittelstandsförderung geplant wurde.

Die Einordnung der USA lässt sich am ehesten über die Akteure vornehmen. Informationen und Materialien zur Informationssicherheit stellen mit der *Federal Communications Commission* sowie der *Small Business Administration* zwei Bundesbehörden zur Verfügung. Die direkte Ansprache im Sinne einer klassischen Mittelstandsförderung findet dann aber eher auf lokaler Ebene statt, wobei lokale Behörden (wie Wirtschaftsförderung und Polizei) mit Unternehmen zusammenarbeiten. Die Ausnahme ist die Initiative *Small Business Corner*, in der drei Bundesbehörden – das *National Institute of Standards and Technology*, die *Small Business Administration* sowie das *Federal Bureau of Insvestigation* – lokale Schulungen anbieten.

Den deutschen Gegebenheiten am nächsten kommen wohl Großbritannien, Österreich und – wenn auch mit einer anderen Herangehensweise – die Niederlande. In allen drei Ländern liegt der Schwerpunkt der Initiativen bei der Mittelstandsförderung, was auch mit der Beteiligung wirtschaftsnaher Einrichtungen korrespondiert, wobei in Österreich die Wirtschaftskammer und in den Niederlanden die Unternehmensverbände vorrangig zu nennen sind. Die Niederlande unterscheiden sich nur insofern, dass die Informationssicherheit in KMU vor allem durch auf Dauer angelegte Initiativen verbessert werden soll.

4.2 Intentionen der untersuchten Initiativen

Die Ausgestaltung einer Initiative ist nicht zuletzt dadurch bestimmt, welche Intention diese hat. Daher widmet sich der zweite Schritt des Vergleichs den

- Zielen der Initiativen im engeren informationstechnologischen Sinne,
- Zielen der Initiativen im Hinblick auf die Dimensionen einer Organisationskultur und
- den durch die Initiative aufgegriffenen Gründen für mangelnde Informationssicherheit in KMU.

Die Ergebnisse dienen dabei nicht nur der Beschreibung der Initiativen, sondern ermöglichen außerdem Hinweise auf deren Effekte.

4.2.1 Ziele im Hinblick auf die Informationssicherheit

Ein wesentliches Merkmal bei der Analyse von Initiativen zur Unterstützung der IT-Sicherheit respektive der Informationssicherheit ist das konkrete informationstechnologische Ziel der Initiative. Allen Initiativen gemein ist, dass sie auf das übergeordnete Ziel einer Verbesserung der Informationssicherheit abzielen. Jedoch formulieren Initiativen zur Informationssicherheit in KMU verschiedene untergeordnete Ziele, um dieses übergeordnete Ziel zu erreichen. Das BSI orientiert sich bei der Analyse der IT-Sicherheit in KMU hinsichtlich der Methodik an den etablierten Standards zur IT-Sicherheit (BSI 2011b), die zur Verbesserung der Informationssicherheit innerhalb der Unternehmen beitragen sollen. Einen ähnlichen Ansatz verfolgen Park et al. (2008) sowie Gillies (2011), indem sie das jeweilige Modell zur Beurteilung des Stands der Informationssicherheit aus den bekannten Standards ableiten. Demzufolge wurden zur Formulierung von geeigneten Merkmalen zur Erfassung der Initiativen auf Grundlage der BSI-Standards 101/102 und der BSI-Grundschutzkataloge in Kombination mit der ISO 27001/2 die in Abbildung 25 aufgeführten Ziele erarbeitet:

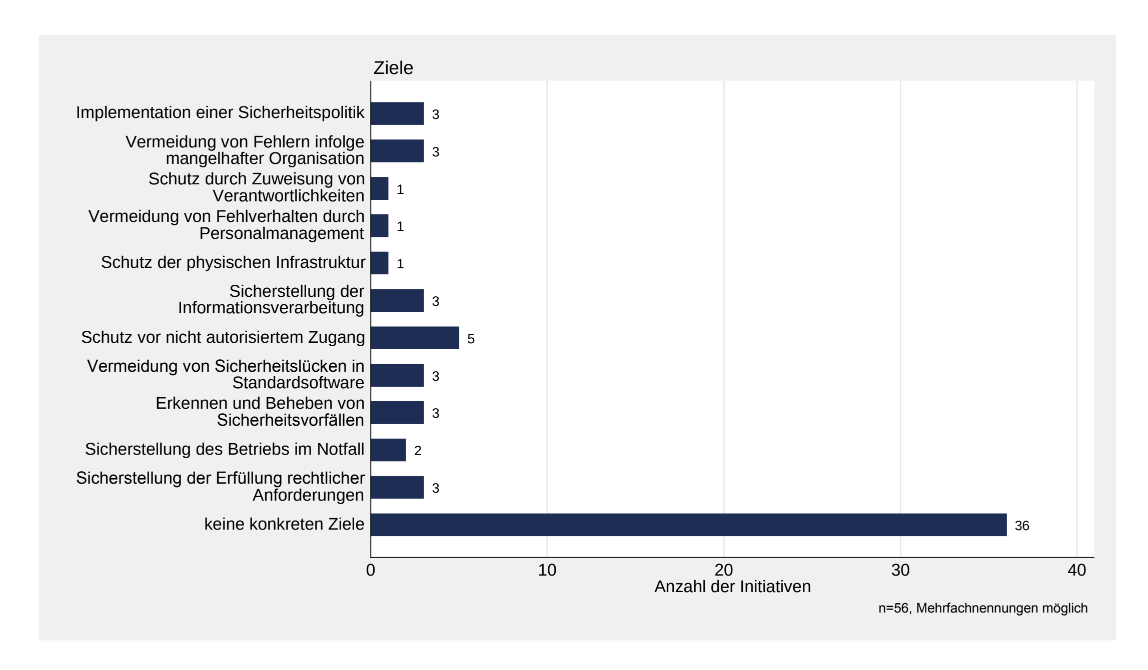


Abbildung 25: Ziele im Hinblick auf die Informationssicherheit im Überblick

Der erste Überblick zeichnet ein irritierendes Bild. Initiativen zur Verbesserung der Informationssicherheit, denen keine konkreten Ziele zuzuordnen sind, erscheinen zunächst einmal schwer vorstellbar. Allerdings bedeutet dies nicht, dass die Initiativen überhaupt keine informationssicherheitsrelevanten Ziele hätten. Vielmehr haben diese Initiativen die Informationssicherheit allgemein zum Thema, verfolgen also – allenfalls unterschiedlich akzentuiert – alle Ziele. Dazu gehören zum einen Kampagnen, Informationsmaterialien und Schulungen, die das Thema Informationssicherheit allgemein vermitteln wollen, also noch keine konkreten Ziele direkt verfolgen, sondern die Unternehmen zu Maßnahmen, die dann einzelne dieser Ziele verfolgen, hinführen. Darüber, inwieweit solche Initiativen hilfreich sind, lässt sich, wie schon oben mit der Kritik von Lacey und James (2010) angesprochen,

streiten. Sicherlich hat eine Initiative ihren Zweck verfehlt, wenn – wie im Falle einer eingestellten Kampagne – selbst der Interviewpartner feststellt, dass es im Nachgang schwer auszumachen soll, ob die Initiative ein konkretes Ziel verfolgt habe.

Zum anderen haben aber auch konkrete Beratungsangebote zunächst einmal kein direkt bestimmbares informationstechnologisches Ziel, da dieses erst im Rahmen der Beratung festgelegt werden kann. Insofern führen auch solche Initiativen das Unternehmen erst dahin, ein konkretes Ziel in Angriff zu nehmen.

Die geringe Spezifität der Initiativen lässt sich in allen untersuchten Ländern beobachten. Deutschland weist nicht zuletzt aufgrund der insgesamt hohen Zahl immerhin sechs Initiativen auf, denen sich konkrete Ziele im Sinne der Informationstechnologie zuordnen lassen. In den anderen Ländern reduziert sich diese Zahl auf maximal eine bis drei Initiativen, wie die nachstehende Abbildung illustriert:

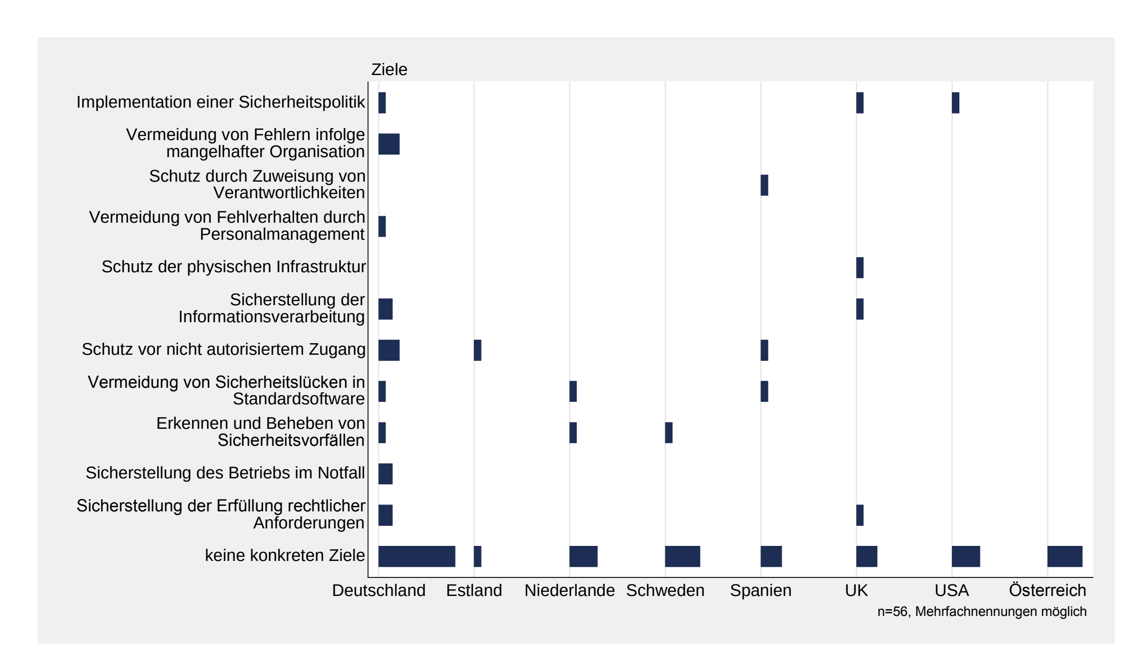


Abbildung 26: Ziele im Hinblick auf die Informationssicherheit

Bei den insgesamt 10 in Frage kommenden Initiativen außerhalb Deutschlands sind keine Schwerpunkte erkennbar. Ebenso unterscheidet sich die Herangehensweise:

- Die Implementierung einer Sicherheitspolitik wird in Deutschland mit einer vereinfachten Zertifizierung (*ISA+*), in Großbritannien mit einem E-Learning-Angebot (*Bob's Business*) und in den USA (*Small Biz Cyber Planner*) mit einer interaktiv zusammengestellten Richtlinie zu erreichen versucht.
- Zur Sicherstellung der Informationsverarbeitung und Datenintegrität führte beziehungsweise führt die deutsche Initiative *IT-Sicherheit in der Hotellerie* Workshops zur Sicherheit von Kreditkartensystemen und die britische Initiative *Business Crime Reduction Center* Beratungen vor Ort durch Polizeibeamte durch.
- Der Schutz vor nicht autorisiertem Zugang war beziehungsweise ist in Deutschland das Thema technologischer Programme (*SimoBIT*, *Trusted Cloud*) sowie der Beratung durch die Handwerkskammern (*komzet@hwk*), in Estland das eines verbindlichen technischen Rahmenwerks zum Datenaustausch (*Estonian Security*

Interoperability Framework) und in Spanien das eines Penetrationstests (*Summer Excercise*).

- Die Erkennung und Behebung von Sicherheitsvorfällen wird in Deutschland durch die Überprüfung von Websites durch die *Initiative-S*, in Schweden durch eine nationale Übung mit wichtigen Unternehmen (Natio*nal Cyber Security Excercise*) und in den Niederlanden mit einem virtuellen Hilfeknopf (*Hulpknop*) gefördert.
- Zur Erfüllung rechtlicher Anforderungen boten in Deutschland ebenfalls die Handwerkskammern in der Initiative *komzet@hwk* und die Workshops für mehr *IT-Sicherheit in der Hotellerie* sowie in Großbritannien wiederum das E-Learning-Angebot *Bob's Business* gezielt Hilfe an.

Nur zur Erkennung von Sicherheitslücken in Standardsoftware bieten sowohl Deutschland als auch Spanien und die Niederlande mit einem CERT dieselbe Lösung an.

4.2.2 Ziele einer Initiative im Hinblick auf die Dimensionen einer Organisationskultur

Die Auswertung im vorangegangenen Kapitel hat ergeben, dass ein großer Teil der Initiativen weniger konkrete Ziele im informationstechnologischen Sinne verfolgt, sondern stärker versucht, ein grundlegendes Bewusstsein für das Thema in der jeweiligen Organisation – in diesem Falle KMU – zu schaffen. Denn die Informationssicherheit eines Unternehmens wird nicht allein durch technische Maßnahmen gewährleistet, sondern ebenso durch eine geeignete Organisationskultur. Dem tragen die Standards, auf deren Grundlage die Merkmale im vorangegangenen Kapitel erarbeitet wurden, auch bereits Rechnung, indem sie die Schaffung einer Sicherheitskultur anmahnen. Allerdings konkretisieren die Standards die Merkmale einer Sicherheitskultur nur im Ansatz, so dass sich der Rückgriff auf die umfangreiche Literatur zu diesem Thema empfiehlt. Dabei sollen die im Folgenden eine Sicherheitskultur konkretisierenden Ziele die im vorangegangenen Kapitel erarbeiteten Ziele nicht ersetzen, sondern lediglich ergänzen. Nach Sichtung der Literatur bieten sich für den Untersuchungszweck vor allem die von Detert et al. (2000) auf Basis einer umfangreichen Auswertung der bis dahin vorhandenen Studien erarbeiteten Dimensionen einer Organisationskultur an. Die Autoren verdichteten aus über 25 untersuchten Konzepten die gefundenen Merkmale zu acht allgemeinen Dimensionen, die sie zum Test auf die Organisation eines Qualitätsmanagements anwendeten. Im Weiteren testeten dann Chia et al. (2002) das Konzept, indem sie die acht Dimensionen zur Beschreibung der Sicherheitskultur einer Organisation adaptierten. Nachstehend werden die Dimensionen sowie deren Adaption für das Thema der Informationssicherheit kurz erläutert.

- Rationalität der Entscheidungen: In einer die Informationssicherheit fördernden Organisationskultur werden Entscheidungen ausschließlich auf Grundlage von Fakten und wissenschaftlichen Methoden getroffen. Initiativen, die zum Beispiel geeignete Bewertungstools zur Verfügung stellen, können hier einen Beitrag leisten.
- Langfristige strategische Orientierung: Obwohl dieses Merkmal auf den ersten Blick einleuchtend erscheint, dürften Unternehmen gerade in Fragen der Sicherheit jedoch vor allem auf aktuelle Bedrohungen reagieren. Dennoch spart eine langfristige Strategie vermutlich Geld und ermöglicht Stabilität.
- Motivation: Mitarbeiter haben keine intrinsische Motivation, Sicherheitsmaßnahmen anzuwenden, und versuchen bei mangelndem Verständnis eher, solche zu umgehen

(Chia et al. 2002). Dem entgegenwirken können Initiativen, die Anreize und Vertrauen schaffen.

- Kontinuität der Optimierung: Ein falsches Sicherheitsverständnis darf nicht dazu führen, dass notwendige Anpassungen unterbleiben. Sicherheit bedeutet nicht, nur Risiken zu vermeiden. Vielmehr ist es das Ziel, die Organisation vorsichtig, aber kontinuierlich weiterzuentwickeln.
- Orientierung an der Arbeit, den Aufgaben und den Mitarbeitern: Sicherheitsmaßnahmen, die an der betrieblichen Wirklichkeit vorbeigehen oder die Mitarbeiter bevormunden, führen zu Produktivitätsverlusten und schwindender Akzeptanz. Eine gute Sicherheitskultur bezieht daher die Mitarbeiter und ihre Arbeit in der Ausgestaltung und Implementierung von Maßnahmen mit ein.
- Kollaboration und Kooperation: Zwar ist jedes einzelne Mitglied einer Organisation für seinen Bereich verantwortlich, die Sicherheit des Unternehmens insgesamt kann so jedoch nicht allein gewährleistet werden. Durch die Zusammenarbeit und den Austausch werden die oftmals bereichsübergreifenden Prozesse sicherer und effizienter.
- Kontrolle, Koordination und Verantwortung: Da die Informationssicherheit nie vollständig sein kann und immer nicht geregelte Umstände eintreten können, bedarf es einer Balance von Verantwortung und Kontrolle sowie der Koordination der – durchaus gewollten – Eigeninitiative der Mitarbeiter.
- Interne und externe Orientierung: In erster Linie ist die Informationssicherheit eines Unternehmens eine interne Angelegenheit. Dennoch hat jedes Unternehmen mehr oder weniger Schnittstellen zu Externen, seien dies Kooperationspartner, Lieferanten, Dienstleister, Behörden oder Kunden. Daher muss das Unternehmen respektive seine Mitarbeiter an diesen Schnittstellen ein Verständnis für die Gefahren besitzen, die dort entstehen könnten, aber auch für die (Sicherheits-/Produktivitäts-)Bedürfnisse externer Beteiligter.

Aufgrund des hohen Anteils von Initiativen, die keine konkreten informationstechnologischen Ziele zum Gegenstand haben, sollte ein erheblicher Anteil der Initiativen – so die Hypothese – aber zumindest einen Einfluss auf diese Dimensionen haben, insbesondere wenn ein Bewusstseinswandel hin zu mehr Informationssicherheit herbeigeführt werden soll. Auf Basis der untersuchten Initiativen lässt sich die Hypothese allerdings nicht verifizieren, wie die nachstehende Abbildung verdeutlicht:

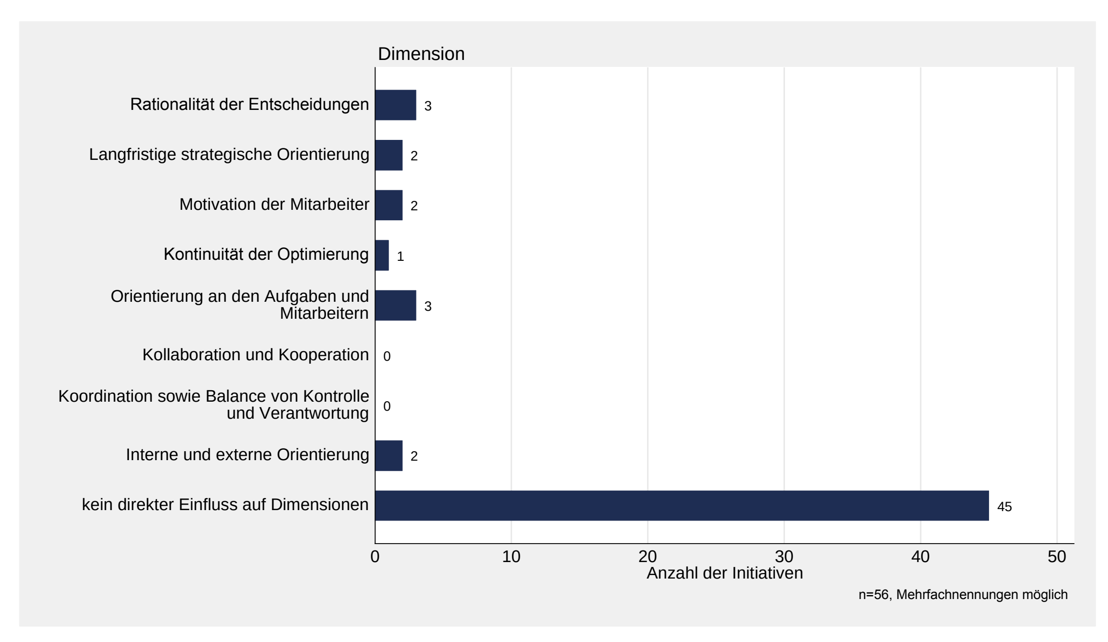


Abbildung 27: Einfluss der Initiativen auf die Dimensionen einer Kultur der Informationssicherheit im Überblick

Auch ohne weitere Auswertung ist zu erkennen, dass ein großer Teil der Initiativen weder konkrete informationstechnologische noch organisationstheoretische Ziele verfolgt. Im Gegenteil, fast alle Initiativen, die einen Einfluss auf die Organisationskultur besitzen, haben auch konkrete informationstechnologische Ziele. Hier zeigt sich das Problem der Initiativen, die KMU lediglich empfehlen, ein Bewusstsein für das Thema Informationssicherheit zu entwickeln, aber die Unternehmen nicht dabei unterstützen, ihre Prozesse entsprechend anzupassen. Einen konkreteren Beitrag zur Organisationsoptimierung bieten hingegen vor allem die Beratungsangebote, die zwar auch im ersten Schritt nur Empfehlungen aussprechen, im zweiten Schritt aber das Unternehmen individuell unterstützen können. Insofern nehmen Initiativen, die a priori keine der Dimensionen betreffen, dann doch einen Einfluss auf die Organisationskultur.

Der Vergleich Deutschlands mit den anderen untersuchten Ländern zeigt, dass die wenigen in Frage kommenden Initiativen überwiegend bereits in Deutschland verortet sind:

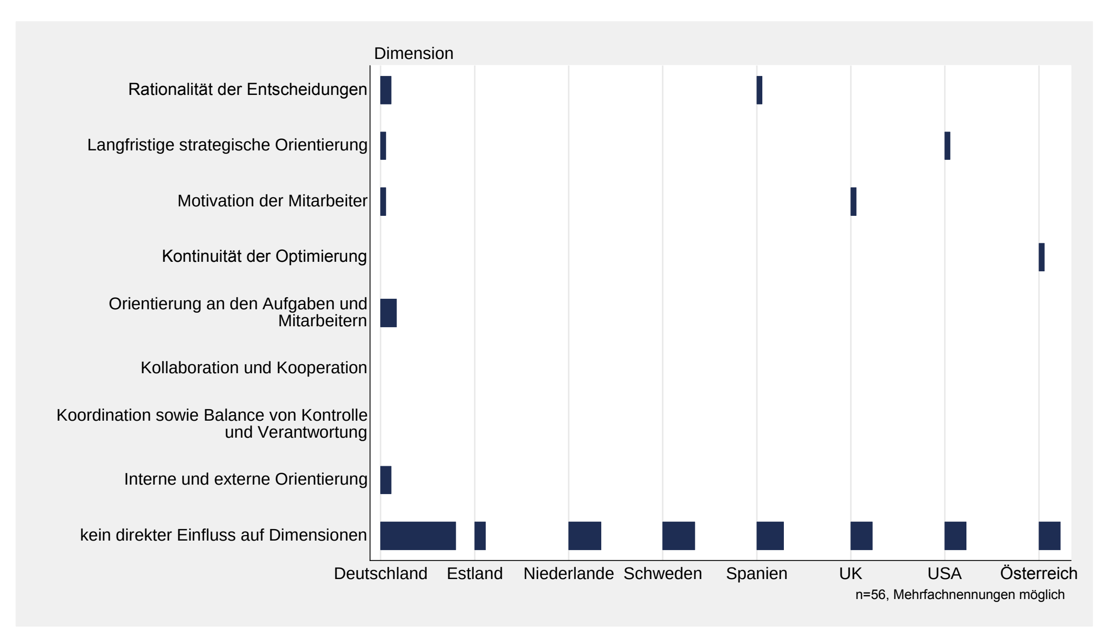


Abbildung 28: Einfluss der Initiativen auf die Dimensionen einer Kultur der Informationssicherheit nach Ländern

Eine interessante Ausnahme ist die zuvor bereits erwähnte Initiative *Bob's Business*, die mit Lernangeboten an Mitarbeiter von KMU einen „behavioural change" herbeizuführen versucht. Der zwar ebenfalls interessante spanische Ansatz, das Entscheidungsverhalten von Unternehmensverantwortlichen durch Penetrationstests zu ändern, konnte – wie in Kapitel 4.1.5 erläutert – bislang nicht auf KMU übertragen werden.

Zu erwähnen bleiben der ebenfalls schon genannte *Small Biz Cyber Planner* in den USA und die Informationsplattform *it-safe.at* in Österreich, die sich besonders der mangelnden Kontinuität von Schulungen annimmt.

4.2.3 Gründe für mangelnde Informationssicherheit in KMU

Eine weitere Möglichkeit, sich der Intention einer Initiative zu nähern, ist zu fragen, welche zu Grunde liegenden Probleme die Initiative aufgreift. Diese Herangehensweise ist deshalb von besonderem Interesse, weil die Verbesserung der Informationssicherheit entscheidend davon abhängt, inwieweit den Gründen für die festgestellten Defizite Rechnung getragen wird. Die Ursachen mangelnder Informationssicherheit in KMU war bereits in der Vergangenheit Gegenstand einer Reihe von Studien, so dass für die Erfassung der Initiativen auf vorhandene empirisch fundierte Erkenntnisse zurückgegriffen werden konnte. Die Auswertung der Studien ergab die in der nachstehenden Abbildung zunächst einmal im Überblick dargestellten neun Gründe:

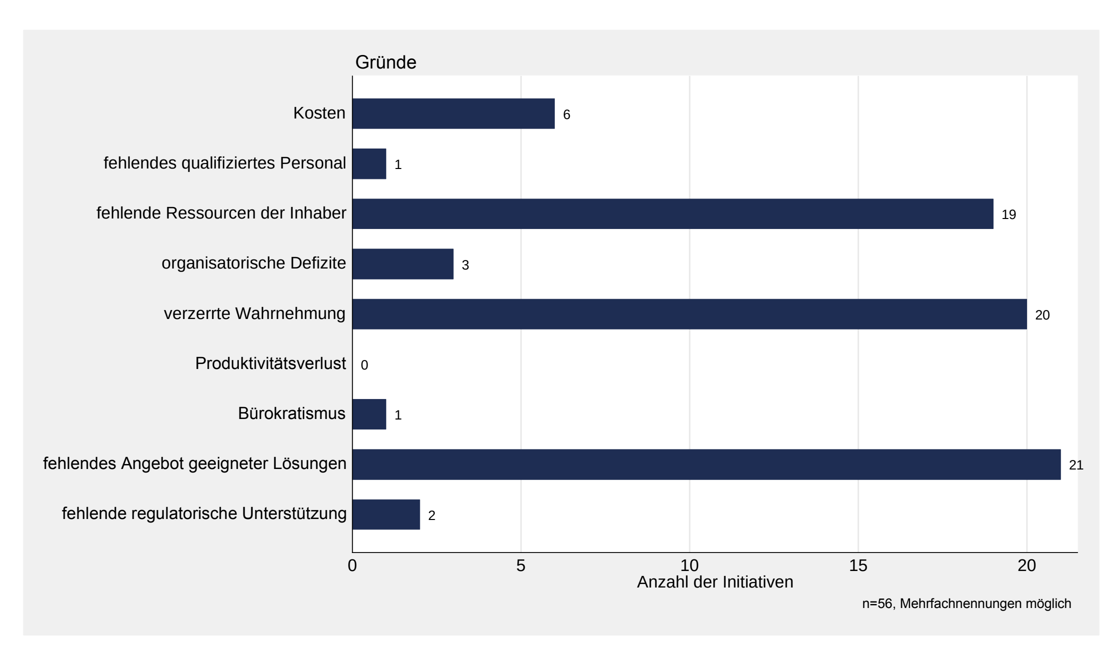


Abbildung 29: Die von den Initiativen aufgegriffenen Gründe für mangelnde Informationssicherheit im Überblick

Wie deutlich zu erkennen, konzentrieren sich die untersuchten Initiativen vornehmlich auf drei Probleme. Allerdings lässt der Vergleich nach Ländern Unterschiede in den Schwerpunkten erkennen:

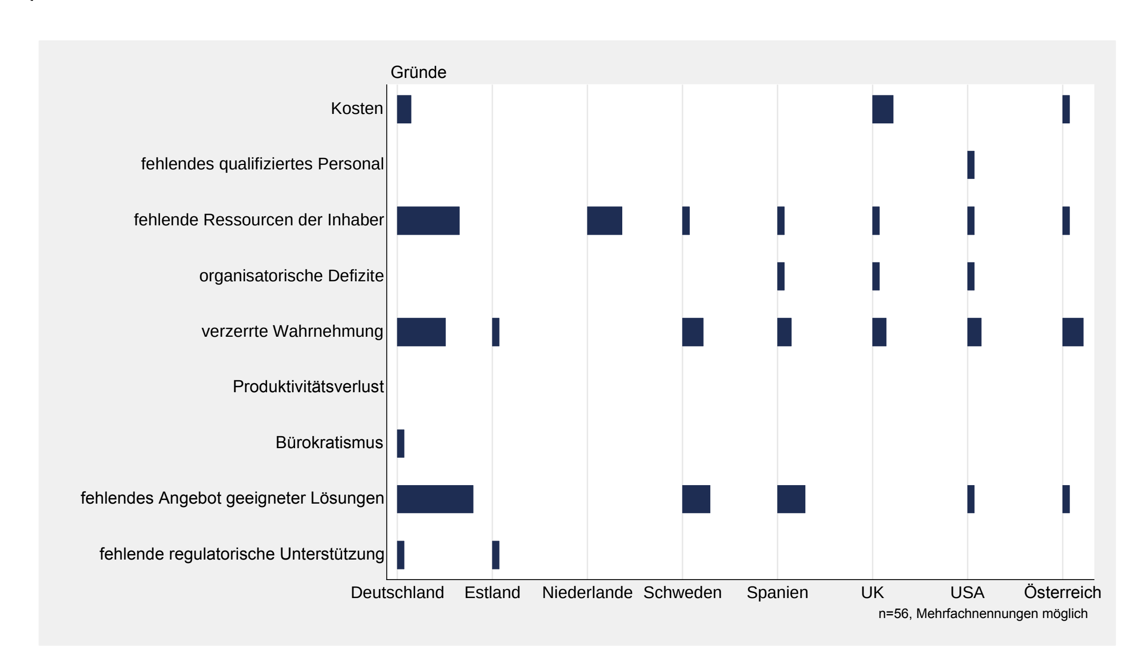


Abbildung 30: Die von den Initiativen aufgegriffenen Gründe für mangelnde Informationssicherheit nach Ländern

Die Verteilung in Deutschland findet sich in dieser Deutlichkeit – nicht zuletzt aufgrund der geringeren Anzahl von Initiativen – in keinem der untersuchten Länder. Vor allem die Niederlande und Großbritannien weichen sichtlich von dieser Verteilung ab. Nur das Problem der verzerrten Wahrnehmung besitzt in allen Ländern – mit Ausnahme der

Niederlande –eine mehr oder weniger hervorgehobene Bedeutung. Im Folgenden werden nun die einzelnen Gründe im Detail erläutert.

Kosten

Es dürfte wenig überraschen, dass eine Vielzahl von Studien die Kosten respektive das Budget für Systeme, Personal und Beratung allgemein als Hemmnis für eine bessere Informationssicherheit nennt[14]. Während dabei in den Untersuchungen von Büllingen und Hillebrand (2012) sowie Reisinger (2013) die Kosten eine bedeutende oder sogar die bedeutendste Rolle spielen, sind in den Auswertungen durch das INTECO (2012a) sowie das Ponemon Institute (2012) andere Gründe wichtiger. Diese Diskrepanz dürfte allerdings zumindest zum Teil in den unterschiedlichen Fragestellungen begründet sein.

Natürlich sind die Kosten einer Sicherheitslösung für alle Unternehmen eine Herausforderung. Aufgrund von gesetzlichen oder internen Regelungen können diese in großen Unternehmen im Verhältnis sogar höher als in KMU sein. So wägen mittelständische Unternehmen ab, inwieweit der erwartete Nutzen aus den Sicherheitsmaßnahmen die zusätzlichen Kosten rechtfertigt[15]. Jedoch stehen der größeren Entscheidungsflexibilität in KMU Skaleneffekte gegenüber, die etwaige Vorteile wieder kompensieren.

Angesichts der Bedeutung der Kosten in den empirischen Untersuchungen erscheint die Zahl der korrespondierenden Initiativen gering. Lediglich Deutschland, Großbritannien und Österreich ermöglichen Leistungen – wozu die Unterstützung zur Implementierung von Standards, die Finanzierung von IT-Dienstleistungen oder Zurverfügungstellung von Technik zur Entwicklung eigener Anwendungen gehören, die ohne die Initiativen in KMU (vermutlich) aufgrund der Kosten nicht verfügbar gewesen wären. Zwar unterstützen auch andere Initiativen die Unternehmen in vielerlei Hinsicht, stellen jedoch das Kostenproblem nicht in den Vordergrund.

Fehlendes qualifiziertes Personal

KMU sehen sich im Hinblick auf die Personalpolitik gleich mit zweierlei Problemen konfrontiert. Zum einen haben alle Unternehmen mit dem Mangel an passend ausgebildeten Mitarbeitern zu kämpfen. Zum anderen ist es KMU aber auch gar nicht möglich, alle Spezialisten einzustellen, die aufgrund der erforderlichen Detailkenntnisse zur Gewährleistung einer umfangreichen Informationssicherheit notwendig wären. Eine dementsprechende Bedeutung kommt dem Personalproblem daher auch in Studien zu[16].

Die Auswertung hat jedoch gezeigt, dass das Management von IT-Personal in KMU bei den untersuchten Angeboten keine Rolle spielt. Die einzige in Frage kommende Initiative in den USA befindet sich derzeit noch im Aufbau und ist in ihrer Ausgestaltung noch zu unbestimmt. Das Problem mangelnder technischer Kompetenz im Unternehmen greifen die Initiativen eher von der Seite des Inhabers auf, womit wir zum folgenden Abschnitt kommen.

[14] Vgl. Gupta und Hammond (2005), Harindranath et al. (2008), Kurki (2006) sowie Lacey und James (2010).
[15] Vgl. Büllingen und Hillebrand (2012) sowie Internet Security Alliance (2013).
[16] Vgl. Büllingen und Hillebrand (2012), Ponemon Institute (2012) sowie Gupta und Hammond (2005).

Fehlende Ressourcen der Inhaber

Ein grundsätzliches Problem insbesondere kleiner Unternehmen besteht in deren Inhaberzentrierung (Ghobakhloo et al. 2011). Inhaber von KMU, die oftmals für alle Funktionsbereiche des Unternehmens selbst zuständig sind, fehlen – sofern sie nicht zufällig IT-Experten sind – die technischen Kenntnisse und die Zeit, sich diese Kenntnisse anzueignen. In Konsequenz führt das mangelnde Wissen zu einem Defizit in der Gewährleistung der Informationssicherheit des Unternehmens[17].

Tatsächlich wurde dieses Problem von vielen Initiativen in allen Ländern aufgegriffen. Dabei fokussieren Initiativen allerdings auf die fehlenden technischen Kompetenzen. Das Problem der zeitlichen Restriktion wird allenfalls am Rande berücksichtigt. Außerdem haben einige Interviewpartner noch auf ein weiteres Hemmnis in diesem Zusammenhang verwiesen. Die Inhaberzentrierung stellt zwar ein prinzipielles Problem über alle Funktionsbereiche hinweg dar, im Bereich der IT erschwert die rasante Entwicklung zusammen mit einem sehr spezifischen Fachwissen den Inhabern die Kompensation etwaiger Defizite. So führen mitunter Angebote, wie zum Beispiel Richtlinien zur Einführung von Standards oder die Beratung von IT-Experten, nicht zum gewünschten Ergebnis, da den Inhabern selbst das Wissen fehlt, um diese Angebote optimal zu nutzen.

Organisatorische Defizite

Nicht immer ist das Fehlen von Geld und Zeit allein für Sicherheitsdefizite verantwortlich. Selbst wenn Technik und Experten verfügbar sind, bedarf es einer gewissen Organisation, ohne die die Instrumente zur IT-Sicherheit nicht durchsetzbar sind[18].

Obwohl Standards zur Vermeidung organisatorischer Defizite vorhanden sind, sind Initiativen zur Unterstützung bei der Beseitigung dieser Defizite Mangelware. Wie schon im Kapitel 4.2.2 erläutert, werden organisatorische Maßnahmen zwar empfohlen, zur Umsetzung derselben fehlen dann aber konkrete Unterstützungsangebote.

Verzerrte Wahrnehmung

Das Ausbleiben von Investitionen in die IT-Sicherheit oder des Outsourcings bei Überlastung des Inhabers folgt zum Teil einem rationalen Kosten-Nutzen-Kalkül. Zum Teil führen die Wissensdefizite der Entscheider jedoch auch zu einer falschen Einschätzung der Bedrohungen und somit zu einem mangelnden Risikobewusstsein[19]. Dasselbe Problem entsteht, wenn die Sicherstellung der Informationssicherheit im Unternehmen in erster Linie als eine technische Aufgabe gesehen wird[20]. In ähnlicher Weise resultieren Überschätzung der eigenen Effizienz sowie Misstrauen infolge fehlenden Wissens beziehungsweise begrenzter Informationsverarbeitungskapazitäten in einer nicht optimalen Nutzung externer Dienstleister oder technischen Lösungen[21].

---

[17] Vgl. Reisinger (2013), INTECO (2012a), Lacey und James (2010), INTECO (2008), Kurki (2006) sowie Gupta und Hammond (2005).
[18] Vgl. Ponemon Institute (2012) sowie Teuteberg (2010).
[19] Vgl. Reisinger (2013), INTECO (2008), Kurki (2006) sowie Gupta und Hammond (2005).
[20] Vgl. INTECO (2010), Lacey und James (2010) sowie Nowey et al. (2009).
[21] Vgl. Eichfelder und Schorn (2012), Ghobakhloo et al. (2011) sowie INTECO (2010).

Die richtige Einschätzung von Bedrohungen, Kosten und Gegenmaßnahmen ist sicherlich die Grundlage einer effizienten Informationssicherheit. Dementsprechend viele Initiativen haben sich bislang diesem Thema gewidmet, wobei sich der größte Teil davon auf das Problem der Unterschätzung möglicher Gefahrenquellen und, mit einigem Abstand folgend, die Unterschätzung der Kosten eines Sicherheitsvorfalls konzentriert. Andere Formen verzerrter Wahrnehmung spielen kaum eine Rolle. Misstrauen gegenüber Externen als Grund für die eigentlich wünschenswerte Inanspruchnahme fachkundiger Dienstleistungen haben allenfalls zwei Initiativen in Deutschland im Blick. Ebenfalls von lediglich zwei Initiativen erkennbar aufgegriffen ist das Problem der Überschätzung der eigenen Effizienz, wobei den – allerdings nur wenigen – Teilnehmern die eigenen Unzulänglichkeiten mittels eines Hacking-Angriffs äußerst plastisch deutlich gemacht wurden.

Produktivitätsverlust

Ein weiterer Grund für das Unterlassen eigentlich wünschenswerter Sicherheitsmaßnahmen liegt in dem schon beschriebenen Konflikt zwischen Funktionalität und Sicherheit (Duscha et al. 2011). Die mangelnde „Usability" ist denn auch ein bedeutendes Hemmnis für österreichische und spanische KMU zur Einführung von Sicherheitslösungen[22]. Infolge führen Produktivitätsverluste nicht nur zu Unmut der Geschäftsführung, sondern auch zur oftmals beklagten fehlenden Akzeptanz der Mitarbeiter.

Obwohl dieses Hemmnis zur Implementierung von Sicherheitslösungen – insbesondere im Hinblick auf die mangelnde E-Mail-Verschlüsselung – leicht nachvollziehbar ist, konnte nicht eine einzige Initiative identifiziert werden, die sich erkennbar des Problems annimmt.

Bürokratismus

Ein oftmals vorgeschlagenes Instrument zur Behebung der oben angesprochenen organisatorischen Defizite ist die Adaption von Standards, zum Beispiel ISO oder BSI. Allerdings kostet deren vollständige Implementierung in einem Unternehmen Zeit und wird von Mitarbeitern mitunter eher als Belastung denn als hilfreich empfunden (Albrechtsen 2007). Vor allem für KMU hat sich die Anwendung solcher Standards als ineffizient erwiesen (Sánchez et al. 2009).

Korrespondierend zu den vorangegangenen Ausführungen ist der Handlungsbedarf hier ebenfalls durchaus erkennbar. Dennoch sind auch Initiativen, die dem Bürokratismus im Unternehmen durch die Einführung informationssicherheitsrelevanter Maßnahmen entgegenwirken – abgesehen von einer Ausnahme in Form der durch das BMWi finanzierten Initiative *ISA+* – nicht identifizierbar.

Fehlendes Angebot geeigneter Lösungen

Zwar existiert am Markt ein großes Angebot an technischen Lösungen, Beratungen und Schulungen, diese gehen jedoch zum Teil an den – oftmals heterogenen – Bedürfnissen

[22] Vgl. Reisinger (2013), INTECO (2012a) sowie INTECO (2010).

mittelständischer Unternehmen vorbei[23]. Die mangelnde Zielgruppenorientierung ist zudem ein Grund, weshalb Kampagneninitiativen mitunter scheitern[24].

Quantitativ wird diesem Problem vor allem in Deutschland Rechnung getragen, wobei allein sieben der elf betreffenden Initiativen vom BMWi im Rahmen der *Initiative IT-Sicherheit in der Wirtschaft* gefördert werden. Über alle Länder hinweg versuchen die Initiativen in erster Linie den Mangel an zielgruppenspezifischen Schulungen sowie – wenn auch in etwas geringerer Zahl – Beratungsleistungen zu beheben. Hingegen konnten Angebote zu technischen Lösungen mit speziellem Fokus auf KMU ausschließlich in Deutschland identifiziert werden. Fünf Initiativen bieten zwar nicht selbst Lösungen an, wollen aber KMU zumindest eine Übersicht dazu geben. Die verbleibenden vier Initiativen in Deutschland und Spanien bieten andere, bis dahin nicht vorhandene Leistungen an, wobei sich die spanischen Bemühungen auf die Verfügbarkeit von Richtlinien in spanischer Sprache beschränken.

Fehlende regulatorische Unterstützung

Einerseits fordern deutsche KMU die Schaffung gesetzlicher Grundlagen (Büllingen und Hillebrand 2012), andererseits beklagen in ähnlichem Ausmaß britische Mittelständler die Komplexität von Regulierungen (Ponemon Institute 2012). Das dem hier zu Grunde liegende Problem gehört eher allgemein zum Thema „Better Regulation" denn zu dem der Informationssicherheit. Dennoch ist es unbestritten, dass einzelne Regulierungen respektive deren Fehlen Einfluss auf die Informationssicherheit von KMU nehmen können. So fanden sich in den Recherchen zumindest eine Initiative in Deutschland zur Unterstützung bei der Erfüllung von Datenschutzanforderungen (*Trusted Cloud*) und eine, bereits zuvor erwähnte, Initiative in Estland, die das Rahmenwerk zum Datenaustausch zur Verfügung stellt. Letztere fokussiert allerdings nicht auf KMU, sondern soll grundsätzlich den Datenaustausch von Unternehmen und Staat sichern. Solche Maßnahmen existieren auch in anderen Ländern, stehen aber dort nicht im Kontext zu Initiativen für mehr Informationssicherheit in KMU.

4.2.4 Zusammenfassung

Zunächst einmal fällt die insgesamt geringe Spezifität der Initiativen hinsichtlich ihrer informationstechnologischen und organisationstheoretischen Ziele auf. Dazu konsistent ist auch der Befund, dass ein erheblicher Anteil der Initiativen vorrangig die Wahrnehmung der Unternehmensverantwortlichen für das Thema Informationssicherheit ändern will. Es würde jedoch den Bemühungen der Länder nicht gerecht werden, wenn diese Erkenntnis dahingehend interpretiert wird, dass die Initiativen zu einem großen Teil beliebig wären. Erstens ist das Vorhandensein eines Bewusstseins für das Thema Informationssicherheit grundlegend für alle weiteren Anstrengungen. Zweitens sind bei genauerer Betrachtung der durch die Initiativen aufgegriffen Gründe mangelnder Informationssicherheit sehr wohl zahlreiche konkrete Ansätze zu erkennen. Hier sind vor allem die Unterstützung der Inhaber bei technischen Belangen sowie zielgruppenorientierte Schulungen und Beratungen zu nennen. Dennoch hat die Auswertung des Einflusses der Initiativen auch ergeben, dass die Angebote noch „weit weg" von den Prozessen in KMU sind. Zum einen ist ein Einfluss der Initiativen

[23] Vgl. Lacey und James (2010) sowie INTECO (2008).
[24] Vgl. Lacey (2010), Harindranath et al. (2008) sowie Albrechtsen (2007).

auf die Organisationskultur nur selten feststellbar, zum anderen deutet insbesondere die nahezu vollständig fehlende Berücksichtigung des Konflikts von Funktionalität und Sicherheit sowie des Problems des Bürokratismus auf noch nicht erschlossene Potenziale hin.

Im folgenden Kapitel wird nun untersucht, mit welchen Ansätzen und Mitteln die Initiativen versuchen, die im Vorangegangenen ausgeführten Ziele zu erreichen beziehungsweise mit welchen Instrumenten die Ursachen für die mangelnde Informationssicherheit angegangen werden.

4.3 Ansätze und Mittel zur Verbesserung der Informationssicherheit

Der dritte Schritt dient dem Vergleich der Ausgestaltung der Initiativen, genauer der gewählten Ansätze und einzelnen eingesetzten Mittel. Dazu wird im Einzelnen untersucht,

- inwieweit die Initiativen Maßnahmenschwerpunkte – in Anlehnung an den BSI-Grundschutzkatalog – aufweisen,
- welche Ressourcen genutzt werden,
- mit welchen Instrumenten die Initiativen im Detail arbeiten und
- welche Gründe mangelnder Informationssicherheit mit den jeweiligen Instrumenten angegangen werden sowie
- abschließend, welche Schnittstellen eventuell für die Arbeit der Initiativen erforderlich sind.

4.3.1 Einordnung der Initiativen in Anlehnung an die Maßnahmen zur Optimierung der Informationssicherheit gemäß BSI-Grundschutzkatalog

Die Implementierung von Sicherheitsstandards stellt konkrete Vorgaben für alle technischen, organisatorischen und prozessualen Aspekte innerhalb einer Organisation bereit. Die Befolgung dieser Vorgaben soll, allgemein ausgedrückt, eine Verbesserung der Informationssicherheit erreichen. Da die hier untersuchten Initiativen ebenso dieses Ziel verfolgen, ist für die Analyse von Interesse, welche Teile der Vorgaben in Bezug zu den Initiativen stehen.

Zu den internationalen Sicherheitsstandards gehören unter anderem Standards wie ISO27001 oder COBIT. Parallel zu diesen Standards existieren nationale Sicherheitsstandards wie beispielweise der IT-Grundschutzkatalog des BSI in Deutschland und das *Österreichische Informationssicherheitshandbuch*, welches die Implementierung von unternehmensspezifischen Informationssicherheitsmanagementsystemen speziell in KMU beschreibt und auf diese Weise die Umsetzung der ISO/IEC 27000 Normenreihe erleichtern soll (Bundeskanzleramt Österreich 2012}. Weitere, speziell für die Bedürfnisse von KMU entwickelte Sicherheitsstandards sind beispielsweise das sogenannte „5S2IS“ Konzept, welches von Gillies (2011) konzipiert wurde.

Grundsätzlich können im Rahmen dieser Studie sowohl die ISO 27001, COBIT, als auch der IT-Grundschutzkatalog des BSI für eine Untersuchung der verschiedenen Initiativen herangezogen werden. In der vorliegenden Studie wird jedoch ausschließlich der IT-Grundschutzkatalog für eine Untersuchung der Initiativen verwendet. Dies ist darin begründet, dass dieser das Thema „Maßnahmen zur Informationssicherheit“ sehr detailliert berücksichtigt, wohingegen andere Standards dieses Thema nicht im Detail behandeln.

Anhand der detaillierten Beschreibung von Maßnahmen ergibt sich so die in Abbildung 31 dargestellte Zuordnung der Initiativen zu den Maßnahmenkatalogen.

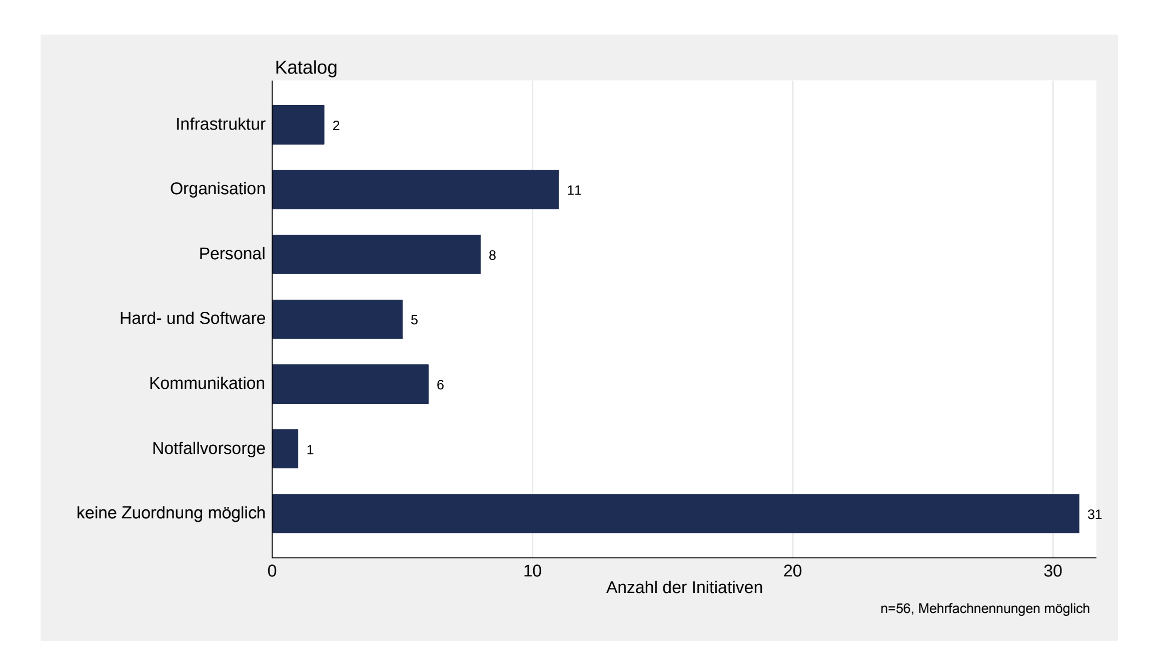


Abbildung 31: Zuordnung der Initiativen zu den Maßnahmenkatalogen des BSI im Überblick

Entsprechend den Auswertungen der Ziele sind die Initiativen auch im Hinblick auf die korrespondierenden Maßnahmen überwiegend unspezifisch. Dabei fällt der Anteil von Initiativen mit einem identifizierbaren Maßnahmenschwerpunkt in Deutschland im Vergleich zu den anderen untersuchten Ländern noch hoch aus:

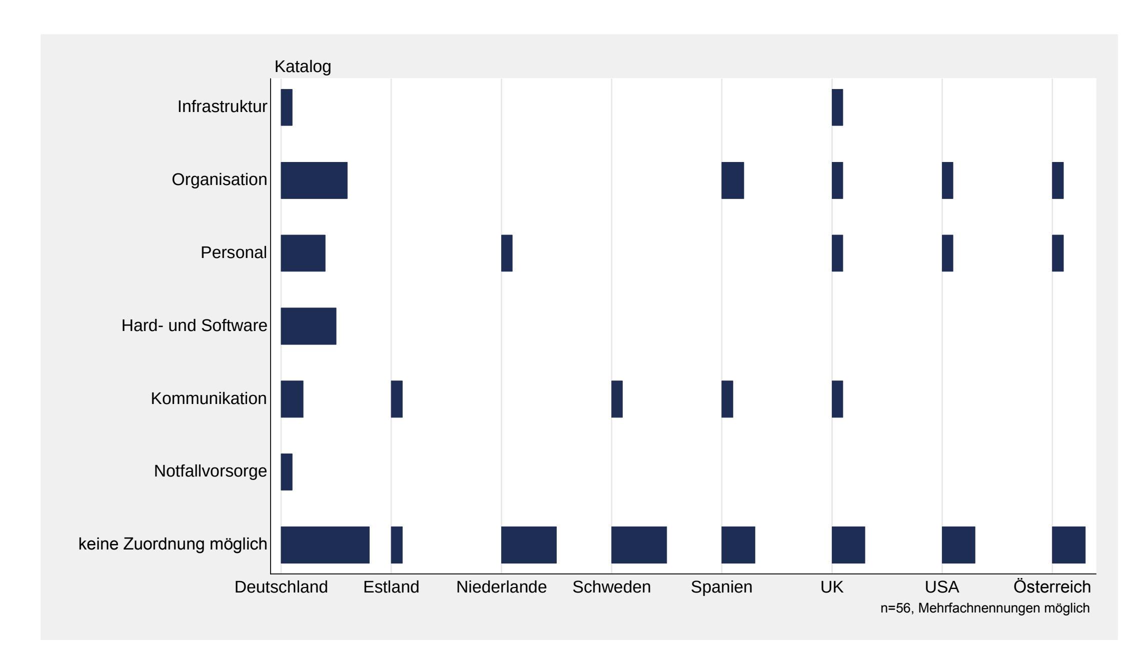


Abbildung 32: Zuordnung der Initiativen zu den Maßnahmenkatalogen des BSI nach Ländern

Angesichts der wenigen in Frage kommenden Initiativen außerhalb Deutschlands ist die Bestimmung von Schwerpunkten kaum möglich. Auffallend ist lediglich, dass Initiativen, die

einen erkennbaren Schwerpunkt in den Bereichen Hard- und Software sowie Notfallvorsorge haben, überhaupt nicht identifiziert werden konnten.

Wie schon in Kapitel 4.2.1 erläutert, bedeutet der Mangel an Spezifität nicht, dass sich aus den Initiativen gar keine Maßnahmen nach dem IT-Grundschutzkatalog ergäben. Selbst eine konkrete Beratung durch einen IT-Experten muss nicht von vornherein auf bestimmte Maßnahmen fokussieren. So stellen die politischen *Innovation Vouchers for Cyber Security* Mittel für eine Beratung vor Ort zur Verfügung, die daraus resultierenden Maßnahmen werden aber erst im Zuge der Beratung festgelegt. Eine andere Vorgehensweise verfolgt das – ebenfalls britische – *Business Crime Reduction Center*, das in der Beratung einen Schwerpunkt beim physischen Schutz der Infrastruktur setzt.

4.3.2 Ressourcen

Initiativen zur Verbesserung der Informationssicherheit greifen auf unterschiedliche Ressourcen zu. Ein Ansatz zur Analyse von Ressourcenverteilungen ist der sogenannte Resourced Based View (RBV). Er definiert fünf mögliche Ressourcentypen. Das Modell umfasst nach Barney (1991) neben finanziellen und Humanressourcen organisatorische, physische und technologische:

- Finanzielle Ressourcen: Finanzielle Mittel werden beispielsweise eingesetzt, um Unternehmen bei der Einführung einer Sicherheitsstrategie zu unterstützen. Hier nicht zu subsumieren sind die finanziellen Fördermittel, die von Seiten des Staates oder auch anderer Einrichtungen der Initiative für ihre Arbeit zur Verfügung gestellt werden.
- Personelle Ressourcen: Personelle Ressourcen bieten in der Regel spezielle Kenntnisse auf dem Gebiet der Informationssicherheit. Möglich ist aber auch, dass die betreffenden Personen nicht selbst die IT-Expertise besitzen, aber als Multiplikatoren ein Unternehmen bei der Suche danach unterstützen.
- Organisatorische Ressourcen: Hierunter werden die Leistungen verstanden, die nicht einzelne Mitarbeiter erbringen, sondern nur die Organisation als Ganzes zur Verfügung stellt. Dazu gehören zum Beispiel die Organisation eines Netzwerks oder die Plattform eines CERTs.
- Physische Ressourcen: Zu dieser Form von Ressourcen gehören beispielsweise anteilig genutzte Serveranlagen.
- Technologische Ressourcen: Im Sinne dieser Studie sind solche Ressourcen in der Regel immaterieller Natur. Es handelt sich um Wissen, das KMU zur Stärkung ihrer Informationssicherheit zur Verfügung gestellt wird. Eine Form von Wissen sind intellektuelle Eigentumsrechte. Durch die freie Nutzung können Unternehmen von Wissen profitieren, das sich KMU sonst in dieser Form finanziell nicht leisten könnten.

Obwohl jede dieser fünf Ressourcen zur Verbesserung der Informationssicherheit zunächst einmal gleich wichtig erscheint, nutzen die untersuchten Initiativen doch zuallererst personelle Ressourcen, wie die folgende Abbildung verdeutlicht:

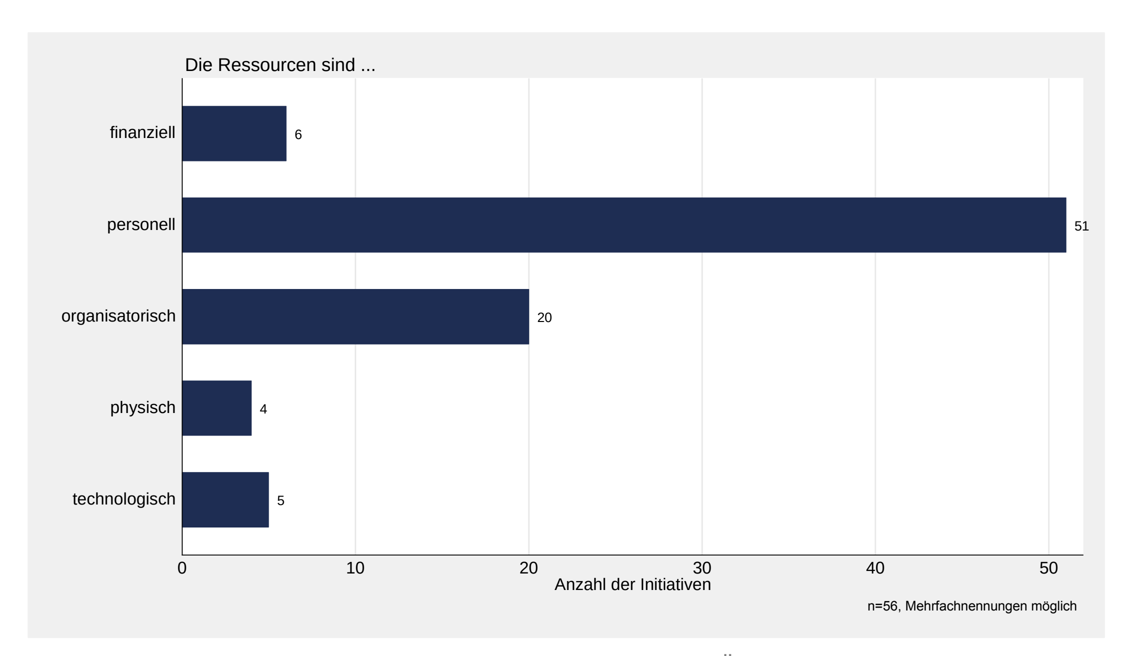


Abbildung 33: Genutzte Ressourcen im Überblick

Dass nahezu jede Initiative ihre Mitarbeiter und Unterstützer in Anspruch nimmt, erscheint dabei weniger verwunderlich, als dass nur die wenigsten Initiativen physische und technologische Ressourcen nutzen. Denn schließlich handelt es sich bei der Informationssicherheit im digitalen Zeitalter um eine technische Herausforderung. Die ohnehin schon geringe Zahl von Initiativen, die finanzielle, physische oder technologische Ressourcen einsetzen, sinkt bei Betrachtung der Initiativen außerhalb Deutschlands nochmals auf lediglich drei:

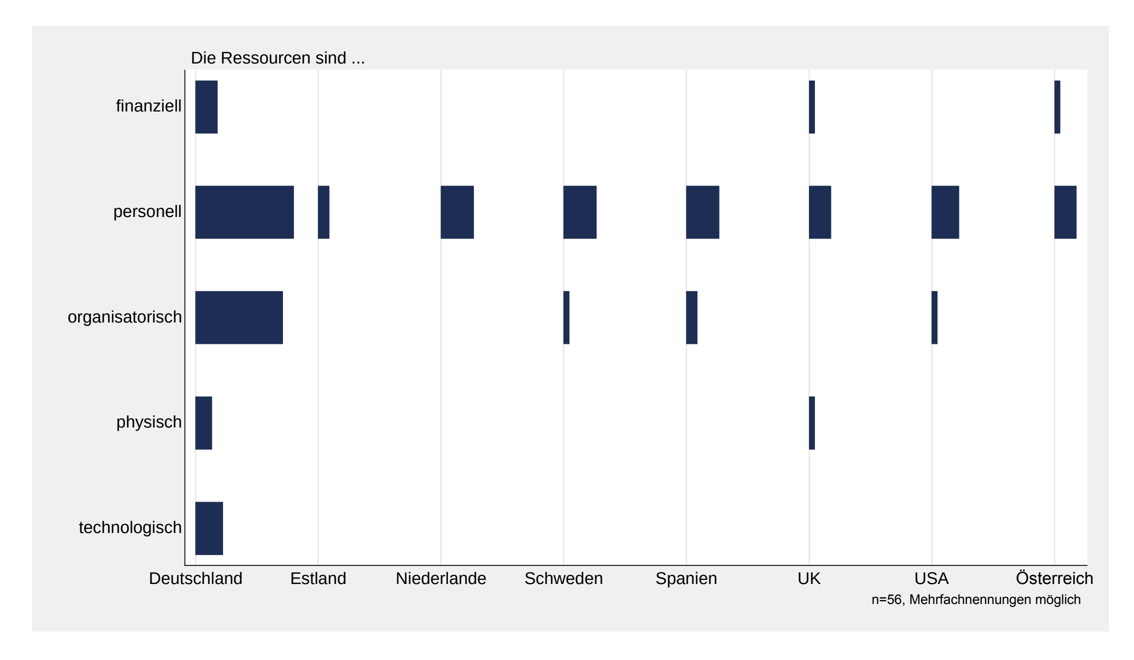


Abbildung 34: Genutzte Ressourcen nach Ländern

Bei zwei dieser Initiativen handelt es sich um Gutscheine für eine Beratung durch IT-Experten und bei einer Initiative um den Aufbau einer Infrastruktur zum E-Learning. Während solche Gutscheine in Deutschland bislang noch nicht eingesetzt wurden, wurde mit

den *Online-Seminaren für IT-Sicherheit in KMU* eine Initiative gefördert, die ebenfalls in der Startphase zunächst einmal die Infrastruktur anschaffen und die Softwaremodule anpassen musste.

4.3.3 Instrumente

Nachdem in den beiden vorangegangenen Kapiteln untersucht wurde, in welchen Bereichen der IT und mit welchen Ressourcengruppen die Initiativen arbeiten, widmet sich dieses Kapitel den genutzten Instrumenten im Detail. Initiativen können sich – wie die Vorrecherche und Literaturauswertung bereits ergaben – grundsätzlich eines breiten Instrumentariums bedienen:

- Informationsmaterial: Das mögliche Angebot reicht von kurzen Ratgebern und Checklisten, zum Beispiel auf Internetseiten, über Erfahrungsberichte und Fallstudien bis hin zu ausführlicheren Richtlinien und Anleitungen.
- Schulungen, Workshops und andere Lernangebote: Eine intensivere und gezieltere Methode der Informationsvermittlung stellen interaktive Lernangebote dar. Diese können die Form von Webinaren (E-Learning), Präsenzkursen oder fachlichen Workshops haben.
- Dienstleistungen: Einige Initiativen gehen über die reine Zurverfügungstellung von Informationen hinaus, indem sie Unternehmen konkrete Dienste anbieten. Hierzu gehören unter anderem die CERTs oder auf das einzelne Unternehmen angepasste Beratungen. Eine einfache Form eines solchen Angebots sind zudem Empfehlungen auf Grundlage von Fragebögen. Eine umfassendere Leistung stellen Angebote dar, die einen lokalen Berater zur Verfügung stellen, der mit den Unternehmen eine maßgeschneiderte Sicherheitslösung ausarbeitet.
- Zuschüsse und Darlehen: Anreize für Verbesserungen der IT-Sicherheit lassen sich, wie auch in anderen Bereichen, gegebenenfalls durch direkte Investitionsbeihilfen, Gutscheine, Steuererleichterungen oder den einfacheren Zugang zu Krediten setzen.
- Belohnungen und Strafen: Solche verhaltenssteuernde Maßnahmen können Zertifizierungen, die das Unternehmen als besonders engagiert in Fragen der Informationssicherheit ausweisen, sein. Mit solchen Zertifizierungen könnten dann auch Erleichterungen bei bestimmten Haftungssachverhalten einhergehen. Umgekehrt könnten Unternehmen bestimmte Leistungen, wie Versicherungspolicen bei fehlendem Engagement vorenthalten bleiben.
- Konferenzen und Kampagnen: Während die voran genannten Angebote sich an Unternehmen richten, die bereits in gewisser Weise für das Thema sensibilisiert sind, haben solche öffentlichkeitswirksamen Maßnahmen in erster Linie Unternehmen und Mitarbeiter als Zielgruppe, denen die Bedeutung der Informationssicherheit noch nicht in dem gewünschten Maße bewusst ist. Neben Konferenzen kommen hier auch Messen, Roadshows oder Medienkampagnen in Betracht.
- Technologieförderung: Der Staat kann Technologien zur Verbesserung der Informationssicherheit in KMU durch die Unterstützung der Entwicklung geeigneter Technologien fördern. Dabei kann die Förderung beispielsweise in Form von Forschungsgeldern oder Investitionsbeihilfen erfolgen.
- Begleitende Instrumente: Ausgestaltung und Erfolg einer Initiative hängen oftmals von den Rahmenbedingungen ab. Beispielsweise kann die technische sowie rechtliche

Standardisierung die Verbreitung von Verschlüsselungstechniken fördern, sofern die Bedürfnisse der interessierten Unternehmen dabei Berücksichtigung finden. Aus diesem einfachen Beispiel lassen sich so für die Erfassung folgende begleitenden Instrumente ableiten:

- Studien und andere Formen der Erfassung der Bedürfnisse von KMU im Hinblick auf die Informationssicherheit,
- Regulierungen mit einem direkten Einfluss auf die Informationssicherheit in KMU (zum Beispiel Gesetze zur elektronischen Signatur und zum Datenschutz),
- Technologien respektive deren Verfügbarkeit zum Einsatz in KMU.

Die Auswertung zeigt, dass tatsächlich ein breites Spektrum an Instrumenten vorzufinden ist. Allerdings nutzen die Initiativen nach dem Eindruck bis hierhin die Instrumente in zum Teil sehr unterschiedlichem Ausmaße:

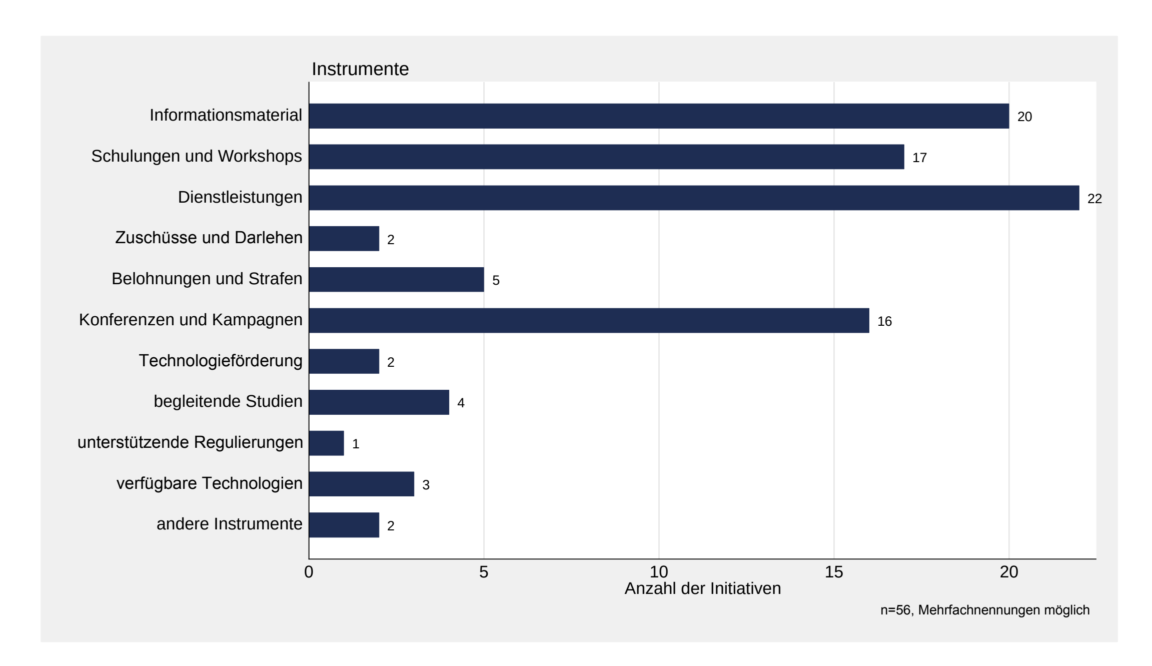


Abbildung 35: Die genutzten Instrumente im Überblick

Die Initiativen konzentrieren sich auf vier Instrumente. Wie schon in der Auswertung zu den Ressourcen gesehen, besitzt die Förderung oder Verfügbarkeit von Technologien keine wesentliche Bedeutung. Ein genauerer Blick auf die Schwerpunkte gibt ein ambivalentes Bild. Etwas mehr als die Hälfte des Informationsmaterials und der Schulungen behandelt Informationssicherheit allgemein. Die verbleibenden Angebote sind hingegen auf KMU respektive einzelne Gruppen von KMU abgestimmt oder entstehen sogar im interaktiven Dialog. Die Dienstleistungen sind tendenziell schon konkreter. Etwas mehr als die Hälfte der betreffenden Initiativen bieten individuelle Analysen und Beratungen an. Die anderen Initiativen erbringen besondere Informationsdienstleistungen, wozu beispielsweise die Auskünfte der CERTs gehören. Initiativen mit öffentlichkeitswirksamen Kampagnen oder Konferenzen haben überwiegend die Bewusstseinsförderung zum Thema. Mitunter, wenn auch nur in wenigen Fällen, wurden im Rahmen von Veranstaltungen auch konkrete technische Lösungen beworben.

Von den insgesamt 56 untersuchten Initiativen konzentrieren sich 40 allein auf diese Schwerpunkte. Die Konzentration wird im internationalen Vergleich nochmals deutlicher:

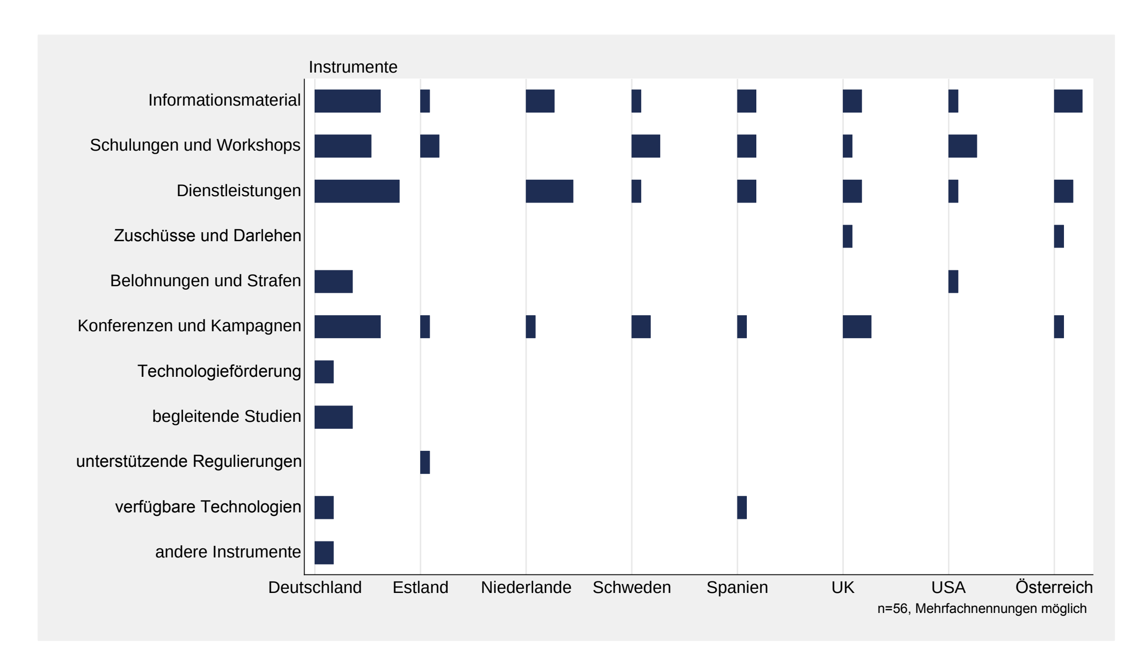


Abbildung 36: Die genutzten Instrumente nach Ländern

Von den 35 außerhalb Deutschlands recherchierten Initiativen nutzen 30 ausschließlich die besagten vier Instrumente. Die Verteilung in den einzelnen Ländern weicht dabei unwesentlich voneinander ab. Lediglich die Niederlande und Österreich scheinen den Wissensbedarf der KMU eher über Dienstleistungen und Informationsmaterialien zu befriedigen denn mittels Schulungen. Dass die USA keine Kampagnen oder Konferenzen nutzen, lässt sich vermutlich durch das Angebot an Schulungen erklären, mit dem speziell KMU erreicht werden sollen. Zwar existieren in den USA auch allgemeine Bewusstseinskampagnen, diese richten sich jedoch nicht explizit an KMU.

4.3.4 Die eingesetzten Instrumente nach den durch die Initiative aufgegriffenen Gründen mangelnder Informationssicherheit in KMU

Die vorangegangenen Ausführungen zeigen, dass sich die in den untersuchten Ländern vorgefundenen Initiativen zur Informationssicherheit nur unzulänglich anhand der Standards zur IT-Sicherheit oder Merkmale einer Organisationskultur – selbst wenn in Publikationen oftmals auf solche verwiesen wird – beschreiben lassen. Im Laufe der Untersuchung sind so die Gründe mangelnder Informationssicherheit sowie die genutzten Instrumente in den Vordergrund gerückt. Von besonderem Interesse ist nun, mit welchen Instrumenten die Initiativen die Gründe für die beobachtbaren Defizite in KMU angehen. Dazu werden einzelne Initiativen respektive die genutzten Instrumente anhand der damit aufgegriffenen Probleme zunächst in der Übersicht in Abbildung 37 illustriert.



Abbildung 37: Instrumente nach den durch die Initiative aufgegriffenen Gründen mangelnder Informationssicherheit

Rein quantitativ betrachtet bemühen sich die Initiativen in den vordersten drei Kategorien,

- fehlende Ressourcen der Inhaber von KMU durch Dienstleistungen zu kompensieren,
- Lernangebote auf die Bedürfnisse von KMU anzupassen und
- Verzerrungen in der Wahrnehmung von Fragen der Informationssicherheit zu korrigieren.

Diese hier über alle Initiativen hinweg ermittelten Schwerpunkte ergeben sich ebenso, wenn nur die Initiativen außerhalb Deutschlands betrachtet werden. Im Folgenden werden nun die einzelnen Ansätze nach den Gründen mangelnder Informationssicherheit gegliedert kurz erläutert.

Kosten

Der direkteste Ansatz, die Kosten zur Schaffung von Informationssicherheit im Unternehmen zu senken, besteht in Zuschüssen, wie sie in Großbritannien durch die *Innovation Vouchers for Cyber Security* gewährt werden. So stellt das *Technology Strategy Board* der britischen Regierung im Rahmen ihres *Innovation Vouchers Scheme* insgesamt £500,000 zur Verfügung, die KMU bis zu einer Höhe von £5,000 beantragen können, um eine Beratung durch IT-Experten zu finanzieren. Die Ausgabe der Gutscheine ist dabei an die Bedingung geknüpft, mit dem Antrag das Vorhaben zu erläutern. Auf diese Weise soll sichergestellt werden, dass die begrenzten Mittel im Hinblick auf ihre Wirkung im Unternehmen möglichst optimal eingesetzt werden. Eine zu den britischen *Innovation Vouchers* vergleichbare Initiative wurde bereits vor einigen Jahren in Österreich mit den *Schecks für Sicherheitschecks* durchgeführt. Es bleibt zu erwähnen, dass die Initiative *go-inno* des BMWi zwar auch mit Innovationsgutscheinen arbeitet, die begünstigten Leistungen bislang jedoch noch keine Maßnahmen zur Verbesserung der Informationssicherheit erfassen.

Darlehen, die zum Beispiel in Deutschland von der Kreditanstalt für Wiederaufbau Unternehmen für Investitionen in erneuerbare Energien zur Verfügung gestellt werden, kommen hingegen – zumindest bislang – in keinem der untersuchten Länder zum Einsatz.

Eine individuelle und aufwändige Beratung vor Ort muss aber nicht zwingend mittels Zuschuss gefördert werden. Die Initiative kann ebenso die Beratung selbst erbringen, sofern die entsprechenden Experten zur Verfügung stehen, wie dies beim britischen *Business Crime Reduction Center* der Fall ist.

Einen etwas anderen Ansatz verfolgen die Initiativen *Bob's Business* in Großbritannien sowie *ISA+* in Deutschland, die KMU den Erwerb einer Zertifizierung erleichtern wollen. Dabei sucht *Bob's Business* dieses Ziel durch ein spezielles E-Learning-Angebot und *ISA+* durch eine auf KMU angepasste Bedarfsanalyse zu erreichen.

Schließlich kann auch die Entwicklung und Zurverfügungstellung von Technologien einen Beitrag zur Kostensenkung leisten. Dieser Ansatz war jedoch nur in Deutschland mit der Initiative *SimoBIT* zu beobachten.

Fehlendes geeignetes Personal

Die geringe respektive nicht vorhandene Beachtung dieses Problems wurde bereits in Kapitel 4.2.3 deutlich. Die einzige in Frage kommende Initiative in den USA verfolgt die Idee,

KMU die Expertise jeweils eines „virtuellen CISO“ zur Verfügung zu stellen. Inwieweit dieser Ansatz allerdings überhaupt umgesetzt wird, ist nach dem derzeitigen Kenntnisstand noch nicht absehbar.

Fehlende Ressourcen der Inhaber

Der naheliegendste Weg, insbesondere die technischen Kompetenzen von Unternehmensinhabern zu stärken, besteht darin, Schulungen, Workshops oder andere Lernformen anzubieten. Allerdings sind die intellektuellen Kapazitäten und die Zeit von Unternehmern begrenzt. Insofern erscheint es plausibel, dass Initiativen fehlende Ressourcen in erster Linie durch ein Angebot von Dienstleistungen auszugleichen suchen. Auf der einen Seite reduzieren Dienstleistungen die Zeit, die ansonsten der Unternehmer selbst aufbringen müsste, auf der anderen Seite erhält der Unternehmer so Zugang zu einer technischen Expertise, die er allein nicht erwerben kann.

Mitunter liegen Schulungen und Dienstleistungen nah beieinander. So bietet das *komzet@hwk* Lehrgänge für Handwerksbetriebe sowie Beratungen im Rahmen der Betriebsbesuche der Handwerkskammern an. Eine andere Möglichkeit ist, dass zunächst Multiplikatoren geschult werden, die dann ihre Klienten (Freie Berufe als Brückenbauer) oder Mitglieder (*IT-Sicherheit im Handwerk*) zumindest im Hinblick auf die Grundlage der Informationssicherheit beraten können. Solche Initiativen konnten jedoch nur in Deutschland beobachtet werden.

Die hier identifizierten Dienstleistungen lassen sich in vier Gruppen zusammenfassen: Beratung der Unternehmen vor Ort (*komzet@hwk*, *Business Crime Reduction Center*), durch interaktiven Dialog zusammengestellte Empfehlungen (*DsiN-Sicherheitscheck*, *Stop Cybercrime/ Cyberscan*, *Bescherm je bedrijf*, *Cyberrad*, *it-safe.at*), aktuelle Warnungen und Sicherheitshinweise (*Bürger-CERT*, *Waarschuwingsdienst.nl*, *INTECO Cert*) sowie technische Analysen und Hilfestellungen (*Initiative-S*).

Die verbleibenden Instrumente wie Informationsmaterial und Kampagnen ergänzten und flankierten lediglich die untersuchten Initiativen.

Organisatorische Defizite

Eine Vielzahl von Initiativen empfiehlt die Einführung von Informationssicherheitsmanagementsystemen auf Basis von Standards wie zum Beispiel dem BSI-Grundschutzkatalog oder der ISO 27001/2. Allerdings unterstützen Initiativen die Unternehmen nur selten, organisatorische Optimierungen tatsächlich vorzunehmen. Für die untersuchten Initiativen trifft dies lediglich in vier Fällen zu. Mit *Bob‘s Business* in Großbritannien sowie die vom *Centro de Ciberseguridad Industrial* angebotenen Schulungen in Spanien unterstützen nur zwei Initiativen KMU durch spezielle Trainings. Hingegen stellt der *Small Biz Cyber Planner* in den USA ähnlich *ISA+* in Deutschland eine auf Basis der Angaben des Unternehmens bedarfsgerechte Sicherheitspolitik zur Verfügung.

Verzerrte Wahrnehmung

Initiativen, die eine gegebenenfalls verzerrte Einschätzung des Unternehmensverantwortlichen zu möglichen Gefahren oder Kosten und Nutzen einzelner Maßnahmen zur Verbesserung der Informationssicherheit korrigieren wollen, lassen sich grob in zwei Gruppen

unterteilen. Die erste Gruppe versucht, Unternehmer überhaupt erst für das Thema zu interessieren. Hierzu dienen in erster Linie allgemein gehaltene Informationsangebote via Internet und öffentlichkeitswirksame Kampagnen, wobei mitunter beide Instrumente komplementär genutzt werden, wie zum Beispiel bei *[m]it Sicherheit* in Deutschland oder *E-Crime Wales* in Großbritannien. Andere Kampagnen hingegen verzichten weitgehend auf die Zurverfügungstellung von Informationen (zum Beispiel die Roadshow *Schutz vor Cyberkriminalität* in Österreich). Umgekehrt wird nicht jedes Informationsangebot mit einer Kampagne beworben. Diese Initiativen wollen zwar auch ein Bewusstsein schaffen, insgesamt stehen aber die Informationen im Vordergrund, wie in den Fällen des „Infoportals" in Schweden, der Seite *Get Safe Online* in Großbritannien oder des *IKT-Sicherheitsportals* in Österreich.

Die zweite Gruppe hat weniger die allgemeine Bewusstseinsbildung zum Ziel als mehr einzelne verzerrte Wahrnehmungen. So soll in Spanien und Schweden in Übungen den Verantwortlichen die Verwundbarkeit ihres Unternehmens bewusst werden. Andere Initiativen – die sich allerdings nur auf Deutschland beschränken – versuchen, KMU für den Rat von Externen zu öffnen (*Freie Berufe als Brückenbauer*), die Gefahren durch Schadsoftware in Internetauftritten aufzudecken (*Initiative-S*) oder die Relation von Nutzen und Kosten einer Investition in IT-Sicherheit realistischer zu beurteilen.

Die Initiativen, die mit Schulungen die Wahrnehmung von Unternehmern ändern wollen, lassen sich in ihrer Mehrzahl nicht ganz so eindeutig einer dieser beiden Gruppen zuordnen. Während die On*line-Seminare für IT-Sicherheit in KMU* und die Workshops im Rahmen der Initiative „IT-Sicherheit in der Hotellerie" in Deutschland sowie durch den *Small Business Corner* angebotenen Schulungen in den USA bereits detailliert einzelne Fragen zur IT-Sicherheit aufgreifen, konzentrieren sich die Lernangebote im Rahmen der Initiativen *Raising Public Awareness about the Information Society* in Estland, *Awareness Raising, Education and Training Program* in Spanien sowie *Cybersecurity for Small Businesses* in den USA noch mehr auf die Bewusstseinsbildung.

Die verschiedenen Angebote wurden respektive werden schließlich bei vier Initiativen noch ergänzt durch kleine Belohnungen in Form eines Siegels (*Initiative-S* in Deutschland und *Cybersecurity for Small Businesses* in den USA), einer begleitenden Sammlung von Fallstudien ([*m]it Sicherheit* in Deutschland) und dem Einsatz des erforderlichen technologischen Instrumentariums für Penetrationstests (*Initiative-S* und die *Summer Excercise* in Spanien).

Bürokratismus

Ein grundsätzlich interessanter Ansatz zur Verhaltenssteuerung besteht in der Belohnung des Unternehmens durch Ausgabe eines „starken" Zertifikates. Stark bedeutet in diesem Zusammenhang, dass das Zertifikat allgemeine Anerkennung findet und im besten Fall sogar rechtliche Bedeutung entfaltet. Zwar existieren mit der ISO 27001/2 oder dem BSI-Grundschutz bereits allgemein anerkannte Zertifizierungen, jedoch ist nicht nur deren Erwerb mit einem erheblichen finanziellen Aufwand verbunden, sondern bedeutet – wie in Kapitel 4.2.3 erläutert – auch die Schaffung bürokratischer Vorgaben, die insbesondere in KMU zu Belastungen führen können, denen kein nachvollziehbarer Nutzen gegenübersteht.

Die einzige, im Rahmen der Erfassung identifizierte Initiative, die sich explizit diesem Problem widmet, ist die bereits erwähnte „Informations-Sicherheits-Analyse, kurz ISA+. Anhand von 65 Fragen mit nach Reifegradmodell angepassten Antwortmöglichkeiten wird

eine speziell für Kleinunternehmen mit weniger als 50 PC-Arbeitsplätzen konzipierte Bedarfsanalyse durchgeführt, auf deren Basis die angemessenen Prozesse für das jeweilige Unternehmen herausgearbeitet werden. Mit Befolgung dieser Prozesse sollen die Unternehmen dann ein Zertifikat erwerben können, das zumindest in absehbarer Zeit allgemeine Anerkennung erlangen soll. Derzeit befindet sich ISA+ aber noch in der Pilotphase.

In ähnlicher Weise wendet sich das britische *Department for Business, Innovation and Skills* mit einem Rahmenwerk (*Cyber Essentials Scheme*), das drei aufeinander aufbauende Zertifizierungen vorsieht, ausdrücklich an KMU. Da die Veröffentlichung dieses Rahmenwerks erst im April dieses Jahres erfolgte, konnte der Ansatz allerdings nicht mehr als Initiative in die ausführliche systematische Erfassung eingehen (BIS 2014a). Der britische Ansatz sieht vor, dass akkreditierte Unternehmen KMU testen und zertifizieren, wobei die Akkreditierung wiederum durch von der Regierung benannte Organisationen erfolgt.

Fehlende geeignete Lösungen

Wie schon in Kapitel 4.2.3 illustriert, scheinen beziehungsweise schienen vor allem geeignete Schulungen bis dahin zu fehlen. Zum Teil handelt es sich dabei um auf die Zielgruppe der KMU angepasste Schulungen. Hierzu gehören in Deutschland die *Online-Seminare für IT-Sicherheit* in KMU und die Workshops der Initiativen *IT-Sicherheit in der Hotellerie* sowie in Spanien die Trainings des *Industrial Cybersecurity Center* und in Schweden die Kurse an der Technischen Universität Stockholm. Der Unterschied bei diesen Initiativen liegt vor allem in den Gebühren. Während die Angebote in Deutschland kostenlos sind, müssen die Unternehmen für die Schulungen in Spanien und Schweden eine Gebühr entrichten. Allerdings endeten die Workshops für die Hotellerie mit Auslaufen der Förderung. Die Schulungen in Schweden hingegen finanzieren sich aus den Gebühren bereits seit 1996. Inwieweit der innovative Ansatz der Deutschen Webinare auch in Zukunft kostenlos bleiben kann, wird sich im Laufe der Jahre erst noch zeigen müssen. Zumindest aktuell plant der Träger auch nach Auslaufen der Förderung keine Gebühren.

Zum Teil verfolgen die in den Recherchen gefundenen Angebote aber auch Ansätze, die sich davon nochmals unterscheiden. So werden die Workshops bei Se*curing our eCity* in den USA nicht allgemein auf KMU angepasst, sondern inhaltlich im Vorfeld abgestimmt, welche spezifischen Anforderungen die Teilnehmer haben. Daraufhin wird dann das Konzept für den ein- bis zweistündigen Workshop aufgebaut. Abschließend findet eine Evaluation mit den Teilnehmern statt, die der Frage nachgeht, inwiefern diese ihr Verhalten geändert haben. Einen ganz anderen Ansatz haben die deutschen Initiativen *Freie Berufe als Brückenbauer* und *IT-Sicherheit im Handwerk* gewählt, indem sie anstelle von KMU direkt Multiplikatoren adressieren, die das erworbene Wissen an KMU weitergeben sollen. Ebenso unterscheiden sich die Veranstaltungen von *nrw.units*, die sich als Reihe gezielt an einzelne Branchen richten. Durch die Veranstaltungen sollen die Spezialisierungsvorteile von kleinen und mittleren IT-Unternehmen herausgestellt und die Hemmschwelle für KMU, eine ansonsten mit Kosten verbundene Beratung im Vorfeld eines Angebots in Anspruch zu nehmen, überwunden werden.

Die verbleibenden Initiativen haben zu einem großen Teil vor allem eine ergänzende Funktion oder geben eine Übersicht zu bestehenden Lösungen beziehungsweise Angeboten. Die Ausnahme stellen die deutschen Technologieprogramme *SimoBIT* und Trusted Cloud dar, die tatsächlich bis dahin fehlenden technischen Lösungen erarbeiteten oder erarbeiten. Wie bereits zuvor erwähnt, scheinen die Verantwortlichen in den anderen untersuchten Ländern keine Notwendigkeit für neue technische Lösungen zu sehen. Die

andere Ausnahme findet sich bei den Initiativen in den Übungen zur Bewältigung von Angriffen, wie sie in Spanien und Schweden durchgeführt wurden. In der Tat war ein solches Angebot bis dahin nicht vorhanden und auch der Ansatz ist durchaus innovativ, jedoch adressieren diese Initiativen zumindest bislang nicht KMU in der Breite, sondern richten sich vielmehr an lediglich eine Hand voll für das Land „kritische“ Unternehmen.

Fehlende regulatorische Unterstützung

Die geringe Bedeutung, die die Initiativen Regulierungen beimessen, wurde bereits in Kapitel 4.2.3 erschöpfend erläutert. Damit soll allerdings keineswegs festgestellt werden, dass eine solche Unterstützung überflüssig wäre. Lediglich liegt die Vermutung nahe, dass die Initiativen in Bezug auf Regulierung eher reaktiv handeln.

4.3.5 Schnittstellen

Das letzte an dieser Stelle betrachtete Kriterium hat in der Informationstechnologie mehrere Bedeutungen. Im technischen Sinne kommt Schnittstellen eine Wandlungsfunktion bei der Umwandlung von Protokollen zu, wie dies beispielsweise bei Netzwerk- und Softwareschnittstellen beziehungsweise -übergängen der Fall ist. Diese Schnittstellen wären jedoch bei den technologischen Instrumenten der Initiativen zu erfassen gewesen. Im Kontext der Untersuchung fungieren Schnittstellen als Übergangspunkt zwischen verschiedenen Akteuren, sind aber selbst keine Akteure oder haben in der Initiative eine Doppelfunktion. Schnittstellen erhalten dabei große Mengen an Informationen, die dort anschließend strukturiert, aufbereitet, kategorisiert und in Form von konkreten Informationen oder auch Handlungsempfehlungen an andere Akteure weitergeleitet werden. Auf diese Weise bietet sich dem Empfänger der Nachricht ein informativer Mehrwert, da er auf Informationen zurückgreifen kann, die ihm ohne die Umwandlung an der entsprechenden Schnittstelle entweder vorenthalten worden wären oder deren Inhalt er ansonsten nur begrenzt hätte nachvollziehen können. Die Vorarbeiten zur Untersuchung deuteten darauf hin, dass die folgenden Schnittstellen eine weiterreichende Bedeutung haben könnten:

- CERTs: Indem CERTs Informationen mit Blick auf IT-Sicherheitsvorfälle (Malware, Spyware, Sicherheitslücken) von Internetdienst- und Netzanbietern erhalten und diese anschließend aufbereiten, können sie konkrete Warnungen, Software- und Verhaltenstipps an die Initiative weitergeben.
- Trust Center: Eine weitere Einrichtung, die eine Schnittstellenfunktion wahrnimmt, sind sogenannte Trust Center. Trust Center bieten für Akteure, die beispielsweise in eine Geschäftsbeziehung treten, einen Zertifizierungsdienst an und fungieren damit als sogenannte vertrauenswürdige dritte Instanz. Indem Trust Center Zertifikate ausstellen, erfolgt eine Bestätigung, dass eine Überprüfung der von einem zum anderen Akteur übermittelten Daten stattgefunden hat.
- Allianzen: Auch die bereits erwähnten Allianzen übernehmen häufig eine Schnittstellenfunktion. Allianzen fungieren als Anlaufstelle für zahlreiche Informationen zu einem spezifischen Thema. Hardware- und Softwarehersteller können Mitglieder von Allianzen sein. Die dort eingehenden Informationen werden von den Mitgliedern der Allianz ausgewertet und anschließend bedarfsgerecht aufbereitet und veröffentlicht. Somit generieren sie für den Empfänger der Informationen einen großen Mehrwert.
- Andere Organisationen: Die Sammlung, Aufbereitung und Weitergabe von sicherheitsrelevanten Informationen ist auch ein Teil des Angebots beispielsweise der Internet-

seiten von Computerzeitschriften. Dabei greifen diese wiederum auf verschiedene andere Quellen – zum Beispiel CERTs Pressemitteilungen von Unternehmen, eigene Erkenntnisse – zurück.

Obwohl in den Vorrecherchen solche Schnittstellen tatsächlich identifiziert werden konnten, so scheinen die Initiativen nach Auswertung aller Länder sich von wenigen Ausnahmen abgesehen selbst zu genügen, worauf die Ergebnisse in Abbildung 38 hindeuten.

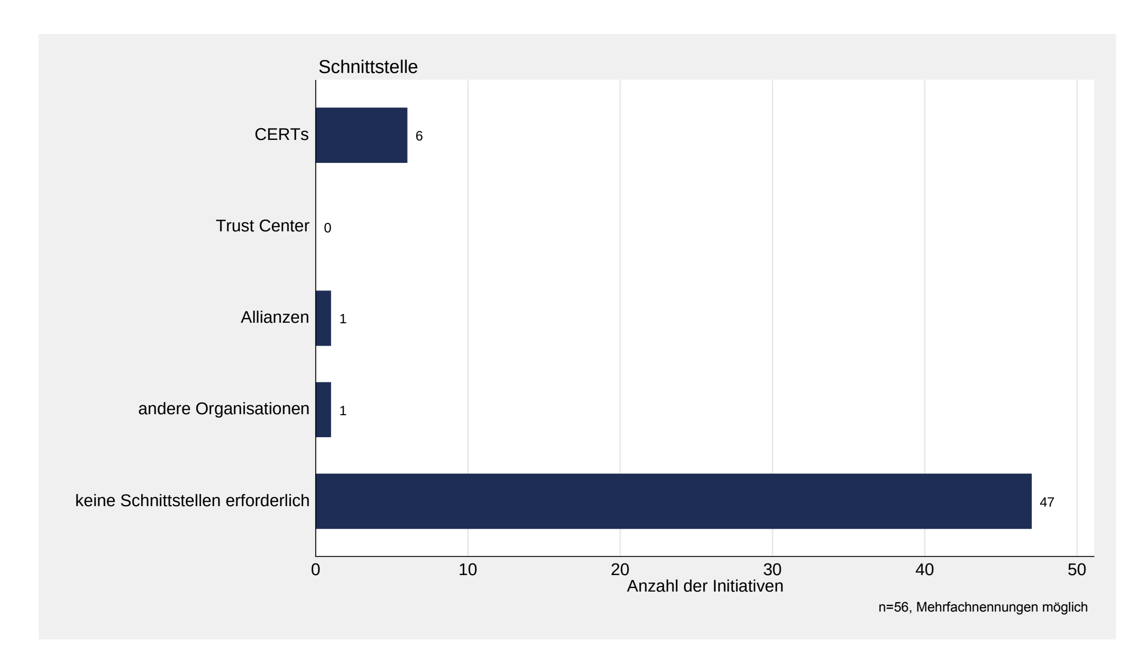


Abbildung 38: Die Schnittstellen der Initiativen im Überblick

Ein Grund für dieses Ergebnis dürfte in den Intentionen und korrespondierenden Instrumenten zu finden sein. So sind laufend aktualisierte technische Informationen zur allgemeinen Bewusstseinsbildung nicht erforderlich. Ebenso wenig benötigen Initiativen die Leistungen von Trust Centers, wenn diese lediglich zur Verschlüsselung mahnen, aber keine konkrete Lösung anbieten. Wie die vorangegangenen Ausführungen schon zeigten, lassen sich dazu kaum Unterschiede zwischen den untersuchten Ländern feststellen:

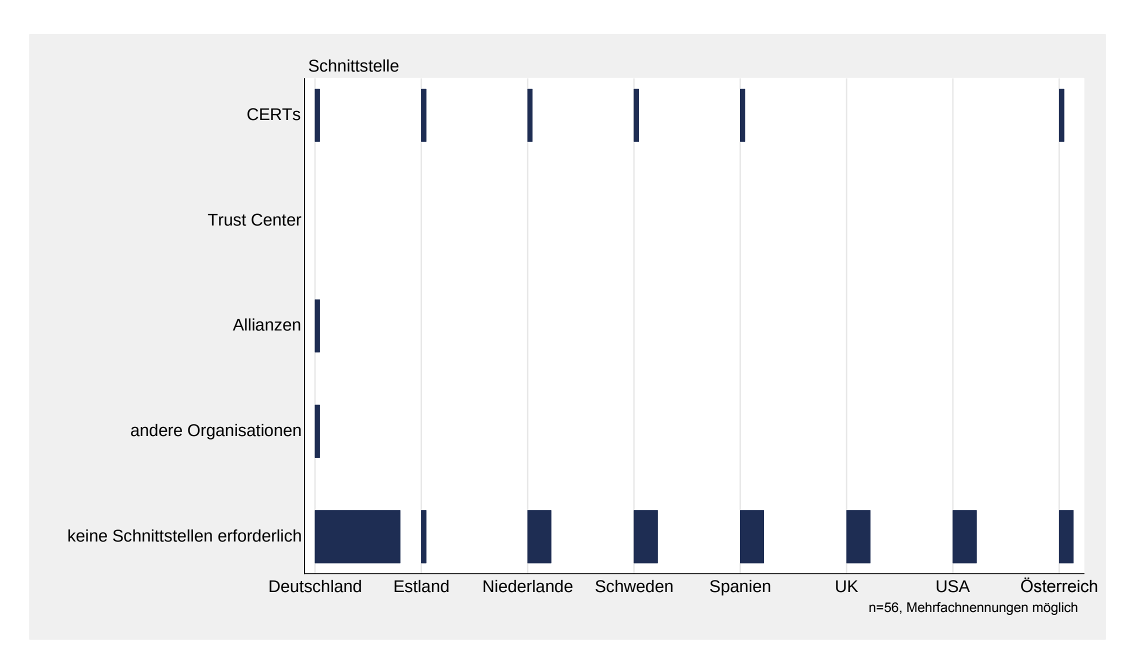


Abbildung 39: Die Schnittstellen der Initiativen nach Ländern

Die Informationen von CERTs wurden immerhin von jeweils einer Initiative in Estland, Schweden und Österreich genutzt. In Deutschland, Spanien und den Niederlanden stellen die CERTs Informationen als Initiative den Unternehmen direkt zur Verfügung.

Andere Informationsquellen werden nur vereinzelt genutzt. Lediglich zwei Initiativen in Deutschland binden Schnittstellen in ihr Angebot ein. Im Fall der Initiative *IT-Sicherheit im Handwerk* sind dies vor allem die Pressemitteilungen von Heise Online, aber auch anderen Portalen. Während diese Mitteilungen eine für die Initiative nicht unbedingt notwendige Leistung darstellen, ist die *Initiative-S* tatsächlich auf die Informationen der Softwareherstel-ler, die sich für diese Initiative in einer Allianz zusammengefunden haben, existenziell angewiesen. Denn nur mit dem Wissen um mögliche Schadsoftware lassen sich die Überprüfungen der Websites der teilnehmenden KMU durchführen.

Auch wenn bislang die vorhandenen Schnittstellen für die Initiativen zur Verbesserung der Informationssicherheit KMU nur marginale Bedeutung haben, könnte hier durchaus ein Potenzial für zukünftige Anstrengungen vorhanden sein. So wird bereits seit längerem im Zusammenhang mit der Initiative *it-safe.at* diskutiert, wie die Informationen des CERT's in Österreich im Hinblick auf die spezifischen Belange von KMU aufbereitet werden könnten.

4.3.6 Zusammenfassung

Die Betrachtung über alle Instrumente hinweg zeigt zunächst einmal, dass konkrete technische Lösungen die Ausnahme darstellen. Angesichts der erheblichen Defizite der KMU insbesondere bei der Verschlüsselung ihrer Kommunikation ist dieser Befund nicht unbedingt zu erwarten gewesen, zumal im Rahmen der Vorarbeiten zur Untersuchung mit der *Initiative-S* ein Beispiel für eine konkrete Unterstützung von KMU identifiziert werden konnte.

Der größte Teil der Initiativen leistet in erster Linie Aufklärungsarbeit, sei es mit Hilfe von Informationsmaterialien, Kampagnen oder Schulungen. Ebenso führt der Teil der Dienstleis-tungen in Form von Beratungsangeboten KMU – im besten Fall – nur an konkrete Lösungen

heran. Insofern ist der britische Ansatz, Gutscheine für eine Beratung nur dann zu gewähren, wenn das Unternehmen zumindest eine Idee hat, welcher Mehrwert sich aus der Förderung für die Informationssicherheit ergeben soll, bereits einen Schritt weiter.

Deutlich seltener zu beobachten sind Initiativen, die unmittelbar einen Einfluss auf die Informationssicherheit des Unternehmens nehmen. In Bezug auf die Dienstleistungen gehören hierzu die Angebote der CERTs – sofern diese den KMU offen stehen – so wie die Penetrationstests und Notfallübungen. Letztere jedoch sind mit Ausnahme der *Initiative-S* nicht aus der Perspektive der Mittelstandsförderung konzipiert, so dass die Mehrzahl der KMU kaum einen Mehrwert aus diesen Initiativen ziehen kann.

Ein weiteres Instrument, das KMU in Zukunft unmittelbar unterstützen könnte, ist die Belohnung in Form eines an die Bedürfnisse von KMU angepassten Zertifikates. Obwohl bei gerade einmal zwei Initiativen – die deutsche *ISA+* sowie das britische *Cyber Essentials Scheme* – noch nicht von einem Trend die Rede sein kann, so orientieren sich diese Initiativen im Vergleich zu den bisherigen doch schon eher an den Prozessen von KMU und entsprechen somit den Wünschen einiger Interviewpartner nach der nunmehr geschaffenen Bewusstseinsbildung, den Bedürfnissen der erreichten KMU nach konkreten Lösungen Rechnung tragen zu können.

4.4 Wirkungen und Nachhaltigkeit der Initiativen

Grundsätzlich beschränkt sich diese Studie – allein aus Gründen der Praktikabilität – auf den Vergleich erfassbarer Merkmale von Initiativen. Hierzu gehören prinzipiell auch Informationen über die Wirkungen einer Initiative, sofern diese denn verfügbar sind. Dabei ist vor allem von Interesse, ob und in welchem Maße eine Initiative die Informationssicherheit der betreffenden Unternehmen verbessern konnte. Im Laufe der Erhebung hat sich jedoch gezeigt, dass die dazu erforderlichen Angaben in der Regel nicht vorliegen. Die wenigen verfügbaren Angaben sind zudem nicht geeignet, um die Wirksamkeit etwa nach der RoSI-Methode (Return on Security Investment) zu beurteilen. Die erhaltenen Auskünfte geben allenfalls Hinweise auf eine mögliche Verbesserung der Informationssicherheit in den Unternehmen.

Ein unmittelbar nachvollziehbarer Erfolg lässt sich wohl am ehesten bei der *Initiative-S* feststellen, da alle rund 17.000 registrierten Unternehmen (Stand März 2014) ihre Websites kontinuierlich prüfen lassen, wobei das Projektteam täglich ein bis zwei Infektionen unschädlich machen kann.

Eine zumindest vergleichsweise hohe Wahrscheinlichkeit, dass eine Initiative tatsächlich einen Einfluss auf die Informationssicherheit des Unternehmens besitzt, kann bei den Abonnenten von CERT-Meldungen angenommen werden, da ein solches Abonnement, wenn es denn schon bestellt wurde, vermutlich auch in den Unternehmen genutzt wird.

Die Wirkungen anderer Instrumente lassen sich nicht immer einschätzen. Dies liegt zum einen daran, dass zum Beispiel zu allgemeinen Informationsangeboten im Internet die Seitenaufrufe protokolliert werden können, die Verwertung der erhaltenen Informationen jedoch unbekannt bleibt. Selbst wenn Unternehmen gezielt Empfehlungen erhalten, muss sich dies nicht unbedingt in konkretem Handeln niederschlagen, wie ein Bericht der niederländischen Organisation CPNI.NL (2013) zeigt. Zum anderen konnten oder wollten

Initiativen nicht immer Auskunft über den Erfolg geben. Außerdem sind Evaluationen, wie sie in Deutschland bei staatlich geförderten Initiativen allein aus haushaltsrechtlichen Gründen üblich sind, in anderen Ländern nicht unbedingt zwingend, vor allem, wenn der Staat die Initiative nur nichtmonetär unterstützt. Die einzige identifizierbare Ausnahme außerhalb Deutschlands stellen die Kurse der Initiative *Securing our eCity* dar. In einer Präsentation der Initiative geben von 54 Befragten 39 an, dass sie die erlernten Konzepte in ihre tägliche Arbeit integrieren konnten. 12 Teilnehmer können immerhin vieles und 3 zumindest einiges von dem Erlernten nutzen. Dieses positive Bild entspricht in etwa auch den Erfahrungen vergleichbarer deutscher Initiativen. Sofern Unternehmen bereits die Bereitschaft zur Teilnahme an Schulungen oder Beratungen haben, scheint auch ein Interesse an der Umsetzung des Erlernten zu bestehen.

Einfacher als Erkenntnisse über die Wirkungen einer Initiative zu erhalten, ist die Ermittlung der erreichten Unternehmen. Dennoch sind entsprechende Angaben auch dazu nur für 21 von insgesamt 56 Initiativen verfügbar, wovon 8 in Deutschland verortet sind. Dies ist darin begründet, dass einige der Initiativen erst kürzlich begonnen haben, keine Erfassung möglich ist (zum Beispiel Websites mit gemischten Angeboten), die Initiative nur indirekt Einfluss auf die Informationssicherheit von KMU hat (zum Beispiel Technologieprogramme) oder schlicht keine Auskunft zu erhalten war (zum Beispiel beim österreichischen *IKT-Sicherheitsportal*).

Aufgrund der großen Zahl an Initiativen, zu denen keine Informationen über die erreichten Unternehmen vorliegen, ist ein internationaler Vergleich nicht möglich. Aber auch die verbleibenden Initiativen sind nur bedingt vergleichbar. So lässt sich die Reichweite einer Internetkampagne nicht mit den Teilnehmerzahlen eines Workshops vergleichen.

Ein Vergleich ist daher allenfalls im Hinblick auf die Reichweite verschiedener Instrumente von Interesse. Dabei fällt auf, dass sich die Reichweiten der meisten Initiativen – wobei selbst die verfügbaren Angaben in vielen Fällen allenfalls als Näherung dienen können – im Promillebereich oder sogar noch darunter bewegen. Die geringsten Teilnehmerzahlen weisen die Notfallübungen in Spanien und Schweden auf, was angesichts der Zielgruppe weniger kritischer Unternehmen sowie des mit der Übung verbundenen Aufwands nicht überraschen kann. Im Gegensatz dazu kann die *Initiative-S,* die zwar eine ähnliche Absicht verfolgt, jedoch auf die Websites der Unternehmen fokussiert und vom Mittelstand her gedacht ist, mit rund 0,6 Prozent (Stand März 2004) eine bereits deutlich höhere Reichweite erzielen.

Schulungen und Beratungen, insbesondere wenn diese speziell angepasst sind, können immer nur eine begrenzte Zahl an Teilnehmern zulassen, besitzen für diese dann aber einen hohen Mehrwert und können über Jahre hinweg auch eine kritische Masse erreichen, wie die Kurse der Technischen Universität Stockholm mit rund 450 teilnehmenden Personen pro Jahr seit 1996 zeigen. Den größten Erfolg in diesem Sinne hatte die Initiative *komzet@hwk*“ die in drei Jahren knapp acht Prozent ihrer Zielgruppe – Handwerksbetriebe im Kammerbezirk Rheinhessen – erreichen konnte.

Ebenfalls eine im Vergleich zu den meisten anderen Initiativen hohe Reichweite erzielen die CERTs in Deutschland und den Niederlanden, deren Abonnentenzahl sich immerhin im einstelligen Prozentbereich bewegt, selbst wenn nicht alle Abonnenten der Gruppe der KMU angehören.

Der beste Wert errechnet sich für das Angebot der Seite it-*safe.at*, über die das *IT-Sicherheitshandbuch* nach Angaben der Wirtschaftskammer Österreich rund 50.000-mal

angefordert wurde, wobei die Zahl der Downloads noch nicht berücksichtigt ist. Dies entspricht auf Grundlage der Zahl der österreichischen KMU nach Eurostat einer Reichweite von rund 16 Prozent. Die Gründe für diesen vergleichsweise hohen Wert lassen sich allenfalls vermuten. So konzentriert sich die Seite auf ein kleines, aber deutlich ersichtliches Angebot. Ein weiterer Grund mag in der Wirtschaftskammer selbst liegen sowie in der Bewerbung des Angebots. Zumindest berichtet der Vertreter der Kammer von einer steigenden Nachfrage nach einzelnen Veranstaltungen.

Zu erwähnen bleiben die zwei Initiativen in Deutschland, die durch die Schulung von Multiplikatoren – zum einen Angehörige der Freien Berufe wie Rechtsanwälte, Wirtschaftsprüfer, Steuer- und Unternehmensberater, zum anderen die Betriebsberater in den Handwerkskammern – den Wirkungsgrad zu erhöhen versuchen.

Insgesamt wurden im Rahmen der Initiative *Freie Berufe als Brückenbauer* 3.008 Teilnehmer geschult. Auf Basis der Evaluation lässt sich – mit aller gebotenen Vorsicht – schätzen, dass rund 80.000 KMU erreicht werden. Die Schätzung beruht auf der Angabe der Teilnehmer über ihre Bereitschaft zur Sensibilisierung ihrer Mandanten (77 Prozent) und der Einschätzung durch die Teilnehmer über die Zahl der erreichbaren Mandanten. Die Evaluation ergab, dass 2014 tatsächlich bereits 44 Prozent der Teilnehmer ihre Mandanten auf das Thema IT-Sicherheit ansprachen.

Die Initiative *IT-Sicherheit im Handwerk* ist derzeit noch in der Phase der Schulungen der Berater, weshalb hier noch keine KMU erreicht wurden. Aufgrund der Nähe der Betriebsberater zu den Mitgliedsunternehmen sowie der Erfahrungen in der Initiative komzet@hwk scheint dieser Ansatz aber durchaus Potenzial zu haben.

Eine Frage, die im Zusammenhang mit den Wirkungen der Initiativen auch gestellt wurde, ist die nach der Nachhaltigkeit. Mit Blick auf den Projektauftrag liegt der Schwerpunkt des Interesses dabei auf den Initiativen, die mit einer staatlichen Förderung initiiert wurden.

Es ist leicht nachvollziehbar, dass Initiativen, die staatliche Zuschüsse gewähren, nicht von Dauer sein können. So wurden denn auch die österreichischen *Schecks für Sicherheitschecks* nach zwei Jahren mangels Budget eingestellt. Auch die britischen I*nnovation Vouchers* verfügen zunächst einmal nur über ein Budget bis 2015, sollen allerdings nach Möglichkeit weitergeführt werden. Dennoch beabsichtigt auch der britische Staat, sich mittelfristig zurückzuziehen in der Hoffnung, bis dahin mit Hilfe der Zuschüsse ein Netz von Geschäftsbeziehungen zwischen IT-Dienstleistern und KMU geschaffen zu haben.

Soweit Auskünfte zur Nachhaltigkeit vorliegen, wird ein großer Teil der Initiativen außerhalb Deutschlands unverändert mit staatlicher Unterstützung fortgeführt. Das einzige Projekt, das sich nach anfänglicher Förderung durch das britische *Department for Business, Innovation & Skills* seit 2008 selbst trägt, ist die mit der deutschen Initiative *Online-Seminare für IT-Sicherheit in KMU* vergleichbaren E-Learning-Plattform *Bob's Business*.

Obwohl das Interesse vorrangig bei anfänglich staatlich finanzierten Initiativen liegt, sollte nicht verschwiegen werden, dass einige Initiativen, wie z.B. *Securing Our eCity*, zwar staatliche Partner haben, aber von Beginn an aus nicht staatlichen Zuwendungen finanziert werden. So ist *Securing Our eCity* als Stiftung organisiert, die durch Partners and Donors getragen wird. Der Vorteil einer solchen Stiftung liegt nicht zuletzt in der überparteilichen Plattform, die es auch zum Teil konkurrierenden Unternehmen erlaubt, finanzielle Mittel und – vor allem – Kompetenzen des Unternehmens einzubringen.

5 Informationssicherheit in ausgesuchten Ländern

Das folgende Kapitel liefert einen detaillierten Überblick zu den untersuchten Ländern in der Europäischen Union und den USA (vgl. dazu Kapitel 3: Auswahl der untersuchten Länder). Die Situation in Deutschland wurde bereits in Kapitel 1 ausführlich dargestellt, weshalb hier auf eine Wiederholung verzichtet wird. Für die verbleibenden sieben Länder werden im Folgenden der Stand der Informationssicherheit und – wo zutreffend – besondere Bedrohungslagen herausgearbeitet. Darüber hinaus wird ein Überblick gegeben über die wesentlichen (teil-)staatlichen Akteure mit Hinblick auf die Informationssicherheit in KMU. Außerdem wird ein Überblick über die wesentlichen Initiativen sowie deren Zielsetzung und Einordnung gegeben. Übergreifend wurden 56 relevante Initiativen in den betrachteten Ländern identifiziert. Zu einer Vielzahl der Initiativen wurden mit lokalen Experten (aus der Privatwirtschaft und staatlichen Stellen) Interviews durchgeführt – die Erkenntnisse sind in die Länderberichte eingeflossen. Um die in den Interviews zugesicherte Vertraulichkeit zu wahren, erfolgt eine namentliche Nennung der Interviewpartner und Quellen einzelner Aussagen nicht.

Bei der Interpretation der in den Länderberichten dargestellten Zahlenwerte, zum Beispiel zur Internetnutzung von Unternehmen, ist zu beachten, dass die referenzierte Datenbank von Eurostat jeweils nur Werte von Unternehmen mit mindestens zehn Beschäftigten ausweist. Für Kleinstunternehmen mit weniger als zehn Beschäftigten existieren keine entsprechenden, flächendeckenden Auswertungen. Auf eine wiederholte Nennung dieses Hinweises im Text wird zugunsten einer besseren Lesbarkeit verzichtet.

5.1 Estland

5.1.1 Kurzüberblick

<table>
<tr><td>Struktur der kleinen und mittelständischen Unternehmen</td><td>
<table>
<tr><th></th><th></th><th></th><th></th></tr>
<tr><td>Mittlere Unternehmen</td><td>1.025</td><td>94.294</td><td>2 Mrd. €</td></tr>
<tr><td>Kleinunternehmen</td><td>5.151</td><td>99.698</td><td>2 Mrd. €</td></tr>
<tr><td>Kleinstunternehmen</td><td>45.697</td><td>107.853</td><td>2 Mrd. €</td></tr>
<tr><td>Summe</td><td>51.872</td><td>301.844</td><td>6 Mrd. €</td></tr>
<tr><td>Anteil an Gesamtwirtschaft</td><td>99,7 Prozent</td><td>78,3 Prozent</td><td>74,4 Prozent</td></tr>
</table>
Quelle: Europäische Kommission (2013d)
</td></tr>
<tr><td>Bedeutung und Stand der Informationssicherheit</td><td>
• Hoher Nutzungsgrad des Internets bei Bürgern und Unternehmen (über EU-Durchschnitt)
• Massiver Cyberangriff auf nationale und private Infrastruktur (Regierung, Banken, Telekommunikation) in Estland im Jahr 2007
</td></tr>
<tr><td>Wesentliche Akteure und Initiativen</td><td>
• Estonian Information System Authority (RIA); betreibt u.a. CERT.ee
• Erste Programme zur Informationssicherheit starteten Ende der 90er Jahre
• Cybersicherheits-Strategie 2008-2013 implementiert; Weiterführung für Zeitraum 2014-2017genehmigt
• Fokus staatlicher Aktivitäten liegt auf dem Schutz kritischer Infrastrukturen
• Wenige Aktivitäten mit Zielgruppe KMU, allenfalls die Kampagne zur Bewusstseinsbildung Raising Public Awareness about the Information Society
</td></tr>
</table>

5.1.2 Bedeutung und Stand der Informationssicherheit

Die Nutzung neuer Technologien und insbesondere des Internets ist in Estland sehr stark ausgeprägt. Der Grundstein hierfür wurde mit dem bereits Ende der 90er Jahre gestarteten Programm *Tiigrihüppe* (estnisch für Tigersprung) und dem Nachfolgeprojekt *Look@world* gelegt. Diese verfolgten das Ziel, die Bevölkerung fit zu machen für die Informationsgesellschaft. Als Ergebnis wird heute unter anderem allen Bürgern per Gesetz der kostenlose Zugang zum Internet garantiert. Um diesen Zugang zu gewährleisten, stehen mehr als 1.100 Hot Spots für den drahtlosen Internetzugang zur Verfügung. Darüber hinaus besteht die Möglichkeit, an einem der mehr als 700 staatlichen Terminals einen Internet-Zugang zu nutzen. Im Jahr 2013 haben 82 Prozent der Esten Dienste im Internet genutzt; mehr als drei Viertel der Haushalte besitzt einen eigenen Breitbandanschluss[25]. Das Vertrauen der Esten in internetbasierte Dienstleistungen ist grundsätzlich sehr hoch. Nur etwa 9 Prozent der Bevölkerung führen bestimmte Aktivitäten wie Onlinebanking oder Onlineshopping aufgrund von Sicherheitsbedenken nicht durch. Hier liegt der EU-Durchschnitt mit 13,9 Prozent weitaus höher. Im Jahr 2007 wurden ca. 98 Prozent der Banktransaktionen in Estland über elektronische Kanäle abgewickelt (Ministry of Defence Estonia 2008).

Ein ähnliches Bild ergibt sich auch bei der Betrachtung der Internetnutzung von Unternehmen. Hier liegt der Anteil der Unternehmen in Estland mit Breitbandzugang (fest und mobil) im Jahr 2013 mit ca. 96 Prozent über dem EU-Durchschnittswert (93 Prozent der Unternehmen). Nahezu die Hälfte aller Unternehmen (48 Prozent) stellte 2011 seinen Beschäftigten tragbare Geräte mit mobilem Breitbandzugang zum Internet zur Verfügung. Die estnischen Unternehmen zeichnen sich darüber hinaus durch hohes Vertrauen bei der Nutzung von Internetdiensten aus. 98 Prozent der Unternehmen, die über einen Internetzugang verfügen, haben bereits 2010 das Internet für Bank- und Finanzdienstleistungen genutzt.

Als Kehrseite des hohen Grades der Vernetzung und der intensiven Internetnutzung wurde Estland im Jahr 2007 Opfer eines großflächig angelegten Cyberangriffs. Der Angriff in Form von Denial-of-Service-Angriffen, die mit Unterbrechungen über einen Zeitraum von zwei Wochen durchgeführt wurden, zielte sowohl auf Regierungs- und Verwaltungsstellen wie auch auf Unternehmen ab. Der Angriff führte dazu, dass wesentliche Teile der Infrastruktur (Öffentliche Verwaltung, Banken, Telekom- und Nachrichtenunternehmen, Energiewirtschaft) lahmgelegt wurden. Seit diesem Angriff hat das Thema Informationssicherheit in Estland auf politischer Ebene deutlich an Bedeutung gewonnen. Hierdurch sieht sich die Regierung Estlands veranlasst, dem Thema der Informationssicherheit bei Bürgern wie Unternehmen eine besondere Priorität einzuräumen.

Trotz der erhöhten Wahrnehmung des Themas Informationssicherheit liegen estnische Unternehmen bei der Umsetzung von Maßnahmen zur Erhöhung der Informationssicherheit im europäischen Vergleich noch deutlich zurück. So weisen beispielsweise erst 11 Prozent der estnischen Unternehmen eine formell definierte Sicherheitsstrategie auf. Der europäische Durchschnitt liegt bei 26 Prozent. Nur etwa die Hälfte dieser Konzepte berücksichtigen die Nichtverfügbarkeit von IKT-Leistungen beziehungsweise Zerstörung oder Verfälschung von Daten durch Angriffe von außen. Die Nutzung von Sicherheitssoftware wie Virenscanner und Firewall liegt in Estland mit 65 Prozenten weit unter dem EU27-Durchschnitt von 84 Prozent. Gleichzeitig liegt die Rate der mit Schadsoftware infizierten Computer mit 42 Prozent weit über dem EU27-Schnitt von 31 Prozent.

---

[25] Sofern nicht anders angegeben, liegt den statistischen Angaben die Eurostat-Datenbank zu Grunde.

Die Recherche im Rahmen des Projektes hat gezeigt, dass in Estland die mangelnde Informationssicherheit bei Unternehmen insbesondere auf die mit der Einführung entsprechender Maßnahmen verbundenen Kosten zurückzuführen ist. Darüber hinaus wurde in den durchgeführten Experteninterviews mehrfach der Mangel an entsprechendem Fachpersonal als Grund genannt. Dies ist jedoch nicht allein eine KMU-spezifische Problematik, sondern als Teil des auch in Estland grundsätzlich herrschenden Fachkräftemangel in Industrie und Technik zu sehen (Germany Trade & Invest 2014). Infolgedessen beschäftigen nur 16 Prozent der KMU in Estland IKT-/IT-Fachleute; der Durchschnitt in Europa liegt bei 20 Prozent. Außerdem werden in nur 11 Prozent der KMU regelmäßig Fortbildungsmaßnahmen zur Erweiterung der IKT-Fertigkeiten angeboten. Um diesem Mangel an IT-Fachkräften langfristig entgegenzuwirken hat Estland im Jahr 2012 ein Programm gestartet, das Kinder bereits ab der ersten Schulklasse mit den Themen IT und Programmieren vertraut machen soll (Jolie O'Dell 2012).

5.1.3 Initiativen zur Unterstützung der Informationssicherheit

Estland zeigt große Bemühungen, bei dem Thema Informationssicherheit auf dem neuesten Stand zu bleiben. Insgesamt weist Estland 26 auf dem Feld der Informationssicherheit aktive Einrichtungen auf (ENISA 2011a). Bereits 2006 wurde die *Estonian Information Sociecty Strategy* ins Leben gerufen (Minister of Economic Affairs and Communications 2006). Im Rahmen dieser nationalen Strategie wurde *Computer Protection 2009* als gemeinsame Aktivität von Estlands größten Banken und Telekommunikationsunternehmen und dem Ministerium für Wirtschaft und Kommunikation gestartet. Ziel dieser Aktivität war es, Estland zur weltweit sichersten Informationsgesellschaft zu machen. Hierzu sollte das Bewusstsein zur Informationssicherheit gestärkt werden und die Bevölkerung in der sicheren Nutzung des Internets unterwiesen werden.

Im Jahr 2008, als Reaktion auf den erwähnten Cyber-Angriff, initiierte das nationale Komitee für die Cyber-Sicherheitsstrategie einen 5-Jahres-Plan mit dem primären Ziel der Verbesserung der Informationssicherheit in Estland, um somit die Anfälligkeit des Cyberspace im Land zu reduzieren (Ministry of Defence Estonia 2008). Das Komitee wurde in der Anfangsphase durch das Verteidigungsministerium in Kooperation mit dem Bildungsministerium, dem Justizministerium, dem Ministerium für Wirtschaft und Kommunikation, dem Innenministerium und dem Außenministerium geführt. Darüber hinaus wurden für die Entwicklung der Strategie Experten aus der Privatwirtschaft herangezogen. Die im Rahmen dieses 5-Jahres-Planes empfohlenen Maßnahmen konzentrierten sich auf die Schwerpunkte „Richtlinien zur Informationssicherheit“, „Bildung“ und „Kooperation“, die dem Ziel einen sicheren Cyberspace für alle Esten zu schaffen, untergeordnet sind (ENISA 2011a). Die Ziele des 5-Jahres-Planes werden durch die Implementierung nationaler Aktionspläne und durch internationale Zusammenarbeit erreicht, wie zum Beispiel in der Aktivität *Cyber Fever 2012*, einer Cyber-Übung, mit der das Krisenmanagement der Regierung auf den Prüfstand gestellt wurde. Nach Auslaufen des 5-Jahres-Plans hat die estnische Regierung im März 2013 die Weiterführung der Cyber-Sicherheitsstrategie für den Zeitraum 2014-2017 genehmigt.

Im Jahr 2011 wurde in Estland ein zentrales Kompetenz- und Koordinationszentrum für die nationale Cybersicherheit gegründet. Dieses ist in der nationalen Behörde *Estonian Information System Authority* (RIA) angesiedelt. Die RIA wiederum ist als Unterabteilung dem Ministerium für Wirtschaft und Kommunikation zugeordnet. Zu den Aufgabengebieten der RIA zählen die Koordination der Entwicklung und Administration der nationalen IT-Systeme, die Steuerung staatlicher Aktivitäten zum Thema Informationssicherheit sowie die Bearbeitung von IT-Sicherheitsvorfällen, die sich in estnischen Netzwerken ereignen. Das estnische CERT ist ebenso Teil der RIA wie eine Abteilung zum Schutz kritischer Infrastruk-

turen. Das zuvor erwähnte Komitee für die Cybersicherheits-Strategie ist im Zentrum für Cybersicherheit in der RIA aufgegangen.

Auch in der universitären Ausbildung spielt das Thema Cybersicherheit in Estland eine große Rolle. So bietet beispielsweise das *Tallinn Institute of Technology* seit einigen Jahren ein Masterprogramm zu Cybersicherheit an, um Unternehmen langfristig gut ausgebildete Fachkräfte zur Verfügung stellen zu können.

Die Aktivitäten zum Thema Informationssicherheit konzentrieren sich in Estland stark auf die Schaffung eines Bewusstseins für das Thema in der allgemeinen Bevölkerung sowie den Schutz kritischer Infrastrukturen. So existiert aktuell nur eine staatliche Initiative in Estland, die KMU adressiert. Bei der Initiative handelt es sich um eine Kampagne zur Förderung des Bewusstseins für Informationssicherheit. Die durch die RIA im November 2007 gestartete Kampagne *Raising Public Awareness about the Information Society* wird überwiegend aus Fördermitteln der Europäischen Union finanziert. Das übergeordnete Ziel der Initiative ist die Entwicklung der Republik Estland zu einer Informationsgesellschaft. Dabei soll insbesondere das Bewusstsein gestärkt werden, dass bei der Nutzung des Internets Risiken entstehen können. Neben Informationskampagnen finden mehrmals im Monat gebührenfreie Schulungen für Unternehmen statt, in denen über die sichere Internetnutzung aufgeklärt wird. Darüber hinaus gibt es spezielle Schulungen für Unternehmen, die an der Entwicklung neuer E-Government-Dienste beteiligt sind. Im Zuge der Initiative konnten bis 2012 etwa 1.000 IT-Spezialisten aus Unternehmen und staatlichen Institutionen geschult werden (Minister of Economic Affairs and Communications 2012). Zur Verbreitung und Weiterleitung der Informationen besteht eine enge Zusammenarbeit mit dem estnischen CERT. Im Zuge der Recherche wurde die Reichweite der Kampagne mit 70 bis 80 Prozent der KMU in Estland beziffert.

Zur Gewährleistung stabiler und sicherer staatlicher IT-Dienste hat das RISO das *Estonian Interoperability Framework* ins Leben gerufen. Hiermit soll nicht nur der sichere Datenaustausch zwischen staatlichen IT-Systemen, sondern auch mit externen privatwirtschaftlichen IT-Systemen erreicht werden. Unternehmen, die beispielsweise E-Government-Dienste für die Regierung entwickeln, sind dazu verpflichtet, diesen Leitfaden als Basis für die Entwicklung sicherer IT-Schnittstellen für die Kommunikation beziehungsweise den Datenaustausch mit staatlichen IT-Systemen zu nutzen. Neben dem Handbuch bietet das RISO auch entsprechende Schulungen für Unternehmen zu dem Thema an.

5.1.4 Wesentliche Erkenntnisse

Estland ist sehr bemüht, die Informationssicherheit stets auf dem aktuellen Stand zu halten. Seit dem Cyber-Angriff im Jahr 2007 hat die Regierung den Ausbau der Informationssicherheit in der Republik nachhaltig forciert. In diesem Kontext ist auch die estnische *Cyber security Strategy* 2008 entstanden. Damals lag die Verantwortung für den Aufbau einer Behörde zur Verbesserung der Informationssicherheit beim Verteidigungsministerium und wurde erst später an das Wirtschaftsministerium übertragen. Die Analyse zeigt jedoch auch, dass das Niveau der Informationssicherheit in kleinen und mittleren Unternehmen in Estland unter dem europäischen Durchschnitt liegt. Staatliche Aktivitäten, die über das reine Informieren von KMU hinausgehen, sind in Estland bislang nicht erkennbar. Der Fokus der allgemeinen Bemühungen zur Verbesserung der Informationssicherheit in Estland liegt auf Aktivitäten, die dem Schutz der kritischen Infrastrukturen und der nationalen Sicherheit dienen. Die Mittelstandsförderung spielt in Estland dagegen keine nennenswerte Rolle. Im Vergleich zu Deutschland lässt sich konstatieren, dass Estland die geringste Ähnlichkeit mit Deutschland aufweist.

5.2 Großbritannien

5.2.1 Kurzüberblick

Struktur der kleinen und mittelständischen Unternehmen

Mittlere Unternehmen	25.727	2.865.963	155 Mrd. €
Kleinunternehmen	145.350	3.227.189	142 Mrd. €
Kleinstunternehmen	1.495.648	3.294.670	177 Mrd. €
Summe	**1.666.725**	**9.387.822**	**473 Mrd. €**
Anteil an Gesamtwirtschaft	99,6 Prozent	52,4 Prozent	49,8 Prozent

Quelle: Europäische Kommission (2013e)

Bedeutung und Stand der Informationssicherheit

- Großbritannien liegt was die Nutzung von IKT-Technologien angeht sowohl bei Privathaushalten als auch bei Unternehmen über dem EU-Durchschnitt
- KMU in Großbritannien sind vielen Angriffen auf ihre IT-Infrastruktur ausgesetzt

Wesentliche Akteure und Initiativen

- Aus der *National Security Strategy* wurde 2010 das *Cyber Security Programme* abgeleitet
- *Department for Business, Innovation and Skills* (BIS) ist der zentrale nationale Akteur im Bereich Informationssicherheit
- Neben den Initiativen auf nationaler Ebene gibt es einige auf regionaler oder lokalem Level, wie zum Beispiel: *Business Crime Reduction Center* oder *E-Crime Wales*

5.2.2 Bedeutung und Stand der Informationssicherheit

Großbritannien liegt bei der Adaption neuer IKT-Technologien sowohl in Privathaushalten als auch in Unternehmen durchweg über dem Schnitt in der Europäischen Union. So besitzen 88 Prozent der Haushalte einen eigenen Internetzugang, 87 Prozent sogar einen Breitbandzugang. Bei der Nutzung von Sozialen Netzwerken weist Großbritannien die zweithöchste Rate in der EU auf – mehr als 56 Prozent der Briten nutzen solche Dienste.

Ein ähnliches Bild ergibt sich bei Betrachtung der britischen Unternehmenslandschaft. 94 Prozent der Unternehmen haben 2012 einen eigenen Internetzugang (Giannakouris und Smihily 2012). Damit liegen sie zwar „nur“ auf Niveau des EU27-Schnitts – ein Unterschied ergibt sich allerdings bei der Betrachtung der eingesetzten Bandbreite. Während 93 Prozent der britischen Unternehmen einen Breitbandzugang besitzen, sind dies im EU27-Schnitt nur 90 Prozent. Laut der Erhebungen des ONS UK (2013b) ist bei kleinen Unternehmen der Anteil an Unternehmen mit Internetzugang zwischen 2007 und 2012 von 87,4 Prozent auf 95,3 Prozent gestiegen. Bei den mittleren Unternehmen ist die Verbreitung noch deutlich ausgeprägter und liegt 2012 bei 99,5 Prozent.

53 Prozent der Beschäftigten nutzen einen Computer mit Internetzugang. Dieser Wert liegt leicht über dem Niveau von Deutschland, aber deutlich über dem EU27-Schnitt. Auch bei der Nutzung mobiler Endgeräte in Unternehmen liegt Großbritannien über dem EU27-Schnitt. So stellten 2012 58,5 Prozent aller Unternehmen ihren Beschäftigten ein tragbares Gerät mit mobilem Breitbandzugang zur Verfügung. Hierbei liegen KMU jedoch deutlich hinter großen Unternehmen zurück. Während bei kleinen beziehungsweise mittleren Unternehmen die Anteile bei 53,6 und 80,0 Prozent liegen, stellen über 90 Prozent der großen Unternehmen ihren Mitarbeitern mobilen Internetzugang zur Verfügung (ONS UK 2013a).

Aktiv sind britische KMU auch bei der Nutzung des Internets für den Kauf und Verkauf von Waren. 57,4 Prozent der kleinen Unternehmen machen Einkäufe über E-Commerce; bei den mittleren Unternehmen sind es sogar 68,2 Prozent (ONS UK 2013a). Dagegen haben im Jahr 2012 17,1 Prozent (kleine Unternehmen) beziehungsweise 23,2 Prozent (mittlere Unternehmen) Waren und Dienstleistungen über ihre Website verkauft.

Kleine und mittelständische Unternehmen in Großbritannien sind sehr stark Angriffen auf ihre IT-Infrastruktur ausgesetzt. So meldeten im Jahr 2013 60 Prozent aller KMU einen Vorfall betreffend ihrer Informationssicherheit. Im Durchschnitt fallen jährlich etwa sechs IT-Sicherheitsvorfälle pro KMU an (BIS 2014b). Beide Werte sind gegenüber dem Vorjahr zwar zurückgegangen – der Fokus der Angreifer scheint sich auf große Unternehmen verlagert zu haben; die Auswirkungen eines Vorfalls nehmen jedoch drastisch zu. So haben sich die durchschnittlichen Kosten eines schweren Vorfalls auf 65.000-115.000 Pfund (entspricht ca. 79.000-140.000 Euro) nahezu verdoppelt. 10 Prozent der Unternehmen, die Opfer eines Angriffs wurden, mussten anschließend die Art ihrer Geschäftstätigkeit ändern. Neben direkten Verlusten beziehungsweise Kosten zur Schadensbehebung entsteht für die betroffenen KMU auch weiterer (nicht-finanzieller) Schaden. So gaben bei einer Befragung durch das Ponemon Institute (2012) 64 Prozent der Unternehmen an, dass ihre Reputation bei Kunden durch einen Datensicherheitsvorfall deutlich gelitten habe. 30 Prozent der befragten Unternehmen waren gezwungen, Mitarbeitern wegen ihres Fehlverhaltens im Kontext der Einhaltung der Informationssicherheit zu kündigen. Die Befragung des BIS (2014b) zeigt, dass 33 Prozent der KMU von unautorisierten Dritten angegriffen wurden, 45 Prozent Opfer eines Virenbefalls wurden und 16 Prozent durch einen Denial-of-Service Angriff betroffen waren. 4 Prozent der KMU wissen, dass Angreifer geistiges Eigentum (Intellectual Property) oder vertrauliche Daten entwendet haben.

Um sich vor Sicherheitsvorfällen zu schützen, haben 29 Prozent der Unternehmen in Großbritannien ein IT-Sicherheitskonzept definiert und liegen damit 2 Prozentpunkte über dem EU27-Durchschnitt (Giannakouris und Smihily 2011). Eine Befragung des BIS (2014b) ergibt, dass sogar 60 Prozent der KMU formal dokumentierte Richtlinien zur Informationssicherheit aufweisen. 39 Prozent der KMU haben Maßnahmen gemäß ISO 27001 ganz oder teilweise implementiert, weitere 19 Prozent planen dies in naher Zukunft zu tun. Um sich vor den Folgen eines Cyberangriffs zu schützen, suchen britische KMU zunehmend auch neue Wege. 2013 hatten bereits 35 Prozent der KMU eine Versicherung abgeschlossen, die im Falle eines Sicherheitsvorfalls die entstandenen Kosten abdeckt (BIS 2014b). Darüber hinaus investieren 69 Prozent der Unternehmen in die Erkennung von Bedrohungen - oder planen dies zu tun. Nachholbedarf gibt es bei britischen Unternehmen bei der Implementierung technischer Maßnahmen für Informationssicherheit. Heute nutzen nur 27 Prozent der Unternehmen eine vollständige Datenverschlüsselung Ponemon Institute (2012). Die Mehrzahl britischer KMU sagt, dass ihre Unternehmen zunehmend Sicherheitsmaßnahmen implementieren. Am häufigsten wurden manuelle Verfahrensanweisungen mit 95 Prozent in den Unternehmen eingeführt, gefolgt von Firewalls (90 Prozent) und Anti-Malware Systemen (89 Prozent) (Ponemon Institute 2012). Um die Informationssicherheit zu verbessern, lassen 54 Prozent der KMU ihre Beschäftigten regelmäßig entsprechende Trainings durchführen (BIS 2014b). Dieser Wert ist gegenüber dem Vorjahr um 6 Prozent gestiegen.

Zusammenfassend konstatiert die vom BIS (2014b) erstellte Studie, dass 59 Prozent der Unternehmen der Überzeugung sind, dass sie ausreichende Fähigkeiten zum Management ihrer Risiken bezüglich Informationssicherheit besitzen. In der gleichen Untersuchung zeigt sich jedoch auch, dass ein Drittel der Unternehmen keinerlei Bewertung ihrer Sicherheitsmaßnahmen vorgenommen hat.

Mit Blick auf die Investitionen, die Unternehmen für IT-Sicherheit aufwenden, lässt sich festhalten, dass rund zwei Drittel der Unternehmen weniger als 10 Prozent ihres IT-Budgets für Sicherheitslösungen ausgegeben haben (Ponemon Institute 2012). Die Hälfte hiervon lag mit ihren Ausgaben sogar bei weniger als 5 Prozent des IT-Budgets. Ähnliche Werte liefert die Befragung des BIS (2014b). Hiernach wenden Unternehmen im Schnitt 10 Prozent ihres IT-Budgets für Informationssicherheit auf. 15 Prozent der KMU setzen sogar 25 Prozent ihres IT-Budgets hierfür ein.

Das größte Gefahrenpotential für die Informationssicherheit geht laut der Untersuchung des Ponemon Institute (2012) von der Nutzung mobiler Endgeräte und der Einbindung privater Endgeräte der Beschäftigten (*Bring-Your-Own-Device*) aus. An zweiter Stelle wird das allgemeine Fehlen von Sicherheitsmaßnahmen für alle Endgeräte aufgeführt. Weiterhin sind Compliance- und Rechtsverstöße und unsichere Drittanbieter, inklusive Anbieter von Cloud-Diensten, als wesentliche Bedrohungen für die Informationssicherheit aufgeführt.

Über alle britischen KMU hinweg kann laut Harindranath et al. (2008) festgestellt werden, dass die Kosten eine wesentliche Hürde bei der Implementierung von Maßnahmen zur Steigerung der IT-Sicherheit darstellen und dies unabhängig von der jeweiligen Organisationsform. Darüber hinaus tragen im IT-Umfeld häufig wenig erfahrene Unternehmensinhaber und Geschäftsführer einen großen Teil dazu bei, dass Investitionen in IT-Sicherheit verzögert werden. Dies resultiert insbesondere daraus, dass es oftmals an IT-Kapazitäten innerhalb der Unternehmen mangelt und so die Vorteile von Maßnahmen zur Informationssicherheit für das Unternehmen nicht klar genug herausgestellt und somit nicht erkannt werden (Harindranath et al. 2008).

5.2.3 Initiativen zur Informationssicherheit

Die 2010 vom *Cabinet Office* und *National Security and Intelligence* veröffentlichte, nationale Sicherheitsstrategie *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (NSS) bildet das übergreifende, strategische Konzept Großbritanniens zum Schutz vor Bedrohungen aufgrund von Terrorismus, Cyberangriffen, internationalen Militärkrisen und Naturkatastrophen (Cabinet Office 2010). Aus der NSS wurde im Rahmen des *Strategic Defence and Security Review* das *Cyber Security Programme* abgeleitet. Dieses Programm stellt über einen Zeitraum von vier Jahren mindestens 650 Millionen Pfund (entspricht ca. 790 Millionen Euro) zur Verfügung, um Großbritanniens Leistungsfähigkeit in Bezug auf den Schutz vor Cyberattacken zu erhöhen. Koordiniert wird das Sicherheitsprogramm vom *Office of Cyber Security & Information Assurance* (OCSIA), das dem *Cabinet Office* zugeordnet ist (ENISA 2011d). Für die Umsetzung der Aktivitäten im Rahmen des nationalen Programms zur Cybersicherheit sind das *Home Office*, *Ministry of Defence* (MoD), *Government Communications Headquarters* (GCHQ), das *Centre for the Protection of National Infrastructure*, das *Foreign & Commonwealth Office* und das *Department for Business, Innovation and Skills* (BIS) zuständig. Durch das OCSIA wurde 2011 auch die nationale *Cyber Security Strategy* publiziert (Cabinet Office 2011). In dieser wird explizit auf die besondere Gefährdung von KMU sowie auf entsprechende Gegenmaßnahmen hingewiesen. Diese strategische Ausrichtung wurde im Dezember 2013 bei einer Überprüfung des Fortschritts der Strategieumsetzung bestätigt (Cabinet Office 2013).

Das BIS ist heute der zentrale nationale staatliche Akteur mit Blick auf Initiativen für die IT-Sicherheit in KMU. Das BIS entstand 2009 durch den Zusammenschluss des *Department for Innovation, Universities and Skills* mit dem *Department for Business, Enterprise and Regulatory Reform*. Es ist unter anderem zuständig für die Förderung von Wachstum und

Innovation in den britischen Unternehmen. Im Rahmen dieser Aufgabenstellung nimmt das Thema Informationssicherheit eine zunehmend wichtigere Stellung ein.

Eine zentrale Initiative, die vom BIS gefördert wird, ist *Get Safe Online*. Diese Bewusstseins-kampage besteht seit 2005 und wird neben dem BIS von weiteren Behörden und Ministerien wie OCSIA, National Crime Agency sowie einer Vielzahl von Unternehmen, zum Beispiel Symantec, Barclays, PayPal, unterstützt. Der Fokus liegt auf der Bereitstellung von Informationsmaterial zum Thema Risiken und Gefahren der Cyberkriminalität für Bürger und KMU. Die Initiative verfolgt das Ziel, Informationen zielgruppengerechter aufzubereiten und zu verteilen. Das Portal gilt mittlerweile als zentrale Anlaufstelle zum Thema Informationssicherheit in Großbritannien.

Im Umfeld des BIS ist auch das *Technology Strategy Board* (TSB) anzusiedeln. Diese öffentliche Körperschaft hat die Förderung von Wachstum und Innovation in den britischen Unternehmen zur Aufgabe. Es unterstützt britische Unternehmen, insbesondere KMU, durch finanzielle Förderung und verschiedene Beratungsleistungen.

Im Jahr 2011 hat das TSB ein bestehendes Programm für Innovationsgutscheine für KMU um Gutscheine für Leistungen im Bereich Informationssicherheit erweitert. Im Rahmen dieser Initiative haben britische KMU die Möglichkeit, Gutscheine in Höhe von 5.000 Pfund zu erhalten. Die Gutscheine können dann für externe Beratungsleistungen eingesetzt werden. Das Programm hat ein jährliches Gesamtvolumen von 500.000 Pfund (Cabinet Office 2011). Somit können bis zu 100 Unternehmen pro Jahr derartige Gutscheine erhalten. Die Vergabe erfolgt über ein einfaches Losverfahren, für das sich Unternehmen über die Beantwortung von Fragen zum Vorhaben qualifizieren können. Zusätzlich zu den Fragen müssen die Unternehmen erläutern, was sie mit den Gutscheinen vorhaben. Die IT-Experten müssen weniger eine fachliche Eignung unter Beweis stellen als mehr ihre wirtschaftlichen Fähigkeiten nachweisen. So soll unter anderem Betrug und Vetternwirtschaft Vorschub geleistet werden.

Ebenfalls durch Förderung des BIS ist die E-Learning-Plattform *Bob‘s Business* entstanden (Lacey und James 2010). Die Förderung durch das BIS lief in den Jahren 2005 bis 2007 – im Anschluss wurde die Initiative in ein privatwirtschaftliches Unternehmen überführt. Neben dem BIS war die *Mid Yorkshire Chamber of Commerce & Industry* bei der Entwicklung der Plattform beteiligt. Ziel von *Bob’s Business* ist es, KMU in die Lage zu versetzen, Standards der Informationssicherheit wie beispielsweise ISO 27001, im eigenen Unternehmen zu etablieren. Dazu bietet die Plattform zahlreiche praxisbezogene und interaktive Übungen an. Das Angebot wird als sehr erfolgreich eingestuft. Während E-Learning-Angebote im Schnitt Beteiligungsraten von rund 10 Prozent erreichen, kommt *Bob’s Business* auf Werte zwischen 70 und 90 Prozent. Darüber hinaus konnte die Plattform seit 2011 ihre Umsätze jährlich verdoppeln (Enterprising Barnsley 17.12.2013).

Ein weiterer Akteur ist das *Government Communications Headquarters* (GCHQ). Das GCHQ ist eine nationale Regierungsbehörde, die mit nachrichten- und sicherheitsdienstlichen Aufgaben, zum Beispiel Fernmeldeaufklärung, betraut ist. Die Unterorganisation *Communications Electronics Security Group* (CESG) hat die Sicherung der elektronischen Kommunikation und Computersysteme Großbritanniens zur Aufgabe. Im Rahmen der Nationalen Sicherheitsstrategie (NSS) wurde festgelegt, dass das GCHQ und insbesondere die CESG zukünftig Dienstleistungen rund um Cybersicherheit, (zum Beispiel Bereitstellung von Warnhinweisen) für britische KMU zur Verfügung stellt. Aus öffentlich zugänglichen Quellen ist eine konkrete Umsetzung dieser Bestrebungen bislang jedoch nicht erkennbar. Bislang wurde lediglich in Zusammenarbeit mit dem CPNI und dem *Council of Registered Ethical*

Security Testers (CREST) eine Zertifizierung von Anbietern für Sicherheitsdienstleistungen, die auch KMU im Falle eines Cyberangriffs in Anspruch nehmen können, ins Leben gerufen (Government Communications Headquarters (GCHQ) 13.08.2013). Darüber hinaus stellt das GCHQ, in Zusammenarbeit mit BIS, CPNI und Cabinet Office, Unternehmen den allgemeinen Leitfaden *10 Steps to Cyber Security* zur Verfügung (GCHQ 2012). Zielgruppe des Leitfadens sind eher große Unternehmen als KMU.

Neben den Initiativen auf nationaler Ebene, gibt es verschiedene Initiativen mit Fokus auf KMU, die auf regionaler beziehungsweise lokaler Ebene angesiedelt sind. Dazu gehört beispielsweise das *Business Crime Reduction Centre* (BCRC), das Unternehmen in der Region Süd-Yorkshire Beratungsleistungen, spezielle Trainings und aktuelle Hinweismeldungen zum Thema Cybersicherheit bietet. Die Beratungsleistungen werden KMU in Form eines Beraters mit IT-Expertise (*Business Advisor)* zur Verfügung gestellt. So können sich KMU, für die es in der Regel zu teuer ist, einen eigenen IT-Sicherheitsbeauftragten zu beschäftigen, gegen die Risiken mangelnder Informationssicherheit rüsten. Bislang konnten bereits mehr als 3.000 KMU mit Beratung unterstützt werden.

Ebenfalls auf regionaler Ebene ist die 2008 gestartete Initiative *E-Crime Wales* angesiedelt. Diese gemeinsame Initiative der vier walisischen Polizeibehörden, nationaler Ministerien beziehungsweise Regierungsbehörden wie das Verteidigungsministerium und Unternehmen aus der IT-Sicherheitsindustrie, zum Beispiel Airbus Defence & Space, Symantec, verfolgt das Ziel KMU mit dem notwendigen Wissen und hilfreichen Werkzeugen zum Schutz vor Cyberkriminalität auszustatten. Neben der Wissensvermittlung über das Onlineportal wird einmal jährlich das *e-Crime Wales Summit*, eine eintägige Konferenz, ausgerichtet.

An verschiedenen britischen Universitäten werden Masterprogramme zum Thema Informations- und Cybersicherheit angeboten: University of Kent, University of Oxford, City University London, De Montfort University Leicester, Queen's University Belfast, Lancaster University, University of Greenwich, University of York und Warwick University.

5.2.4 Wesentliche Erkenntnisse

In Großbritannien liegt der Schwerpunkt bei den Initiativen zur Förderung der Informationssicherheit im Bereich der Mittelstandspolitik. Obwohl im Zuge der Diskussionen um die Aktivitäten der US-amerikanischen *National Security Agency* (NSA) auch das britische GCHQ in die deutsche Nachrichtenberichtserstattung geriet, sind in diesem Kontext keine Maßnahmen zur Verfolgung geostrategischer Ziele erkennbar. Der starke Mittelstandsbezug liegt vermutlich an dem Engagement der unternehmensnahen Einrichtungen, die mit regionalen Partnern vor Ort einen direkten Bezug zu den ansässigen Unternehmen haben. Das BIS als zentraler staatlicher Akteur im Bereich Informationssicherheit hat mit *Get Safe Online* eine zentrale Anlaufstelle etabliert. Von den vorhandenen Initiativen können häufig auch größere Unternehmen profitieren, so dass sich Initiativen nicht immer ausschließlich nur an KMU richten.

5.3 Niederlande

5.3.1 Kurzüberblick

Struktur der kleinen und mittelständischen Unternehmen

Mittlere Unternehmen	8.497	1.012.041	67 Mrd. €
Kleinunternehmen	45.079	1.102.544	60 Mrd. €
Kleinstunternehmen	602.149	1.438.484	62 Mrd. €
Summe	**655.724**	**3.553.069**	**189 Mrd. €**
Anteil an Gesamtwirtschaft	99,8 Prozent	66,3 Prozent	63,8 Prozent

Quelle: Europäische Kommission (2013b)

Bedeutung und Stand der Informationssicherheit

- Bei den Niederlanden handelt es sich um ein sehr IT-affines Land, das bei der Adaption neuer Technologien in Europa eine Vorreiterrolle einnimmt
- Sowohl Privatpersonen als auch Unternehmen weisen eine überdurchschnittliche Nutzung des Internets auf
- Niederländische Unternehmen sind überdurchschnittlich häufig von Störungen ihrer IT betroffen
- Trotz der erhöhten Gefährdung ihrer Systeme liegen niederländische Unternehmen bei der Implementierung einer Sicherheitspolitik im europäischen Durchschnitt

Wesentliche Akteure und Initiativen

- *Ministry of Security and Justice*
- *MKB Nederland* (Verband niederländischer KMU)
- *Digibewust* (Partnerschaft aus Staat, Wirtschaft und Zivilgesellschaft)
- Zentral ist die Website www.stopcybercrime.nu auf der verschiedene weitere Initiativen angeboten werden: *Hulpknop* (Notfallknopf), *Cyberscan* und *Cyberrad*

5.3.2 Bedeutung und Stand der Informationssicherheit

Die Niederlande sind in Europa führend in Bezug auf die Adaption technologischer Trends und der Nutzung von IKT-Werkzeugen. Sie besitzen darüber hinaus einen sehr konkurrenzstarken Internetmarkt, stellen einen internationalen Internetknotenpunkt dar und weisen höchste Raten bei der Internetnutzung auf (Ministry of Security and Justice Netherlands 2013).

95 Prozent der niederländischen Haushalte besitzen einen eigenen Internetzugang, 87 Prozent haben sogar einen Breitbandzugang. Das Niveau der Internetkenntnisse liegt bei den Nutzern deutlich über dem EU-Schnitt – es werden vielfach auch fortgeschrittene Dienste genutzt. 83 Prozent der Niederländer nutzen (fast) täglich das Internet – ein Spitzenwert in der EU. Auch bei der Nutzung von Sicherheitssoftware liegen die Niederländer im EU-Vergleich ganz vorne: 96 Prozent der Niederländer haben Virenscanner, Firewall usw. im Einsatz (Eurostat 08.02.2011). Folglich liegt die Rate der infizierten Rechner in den Niederlanden mit 23 Prozent auch deutlich unter dem EU-Schnitt von 31 Prozent.

Bei den niederländischen Unternehmen liegt die Quote der eigenen Internetzugänge bei 100 Prozent, 96 Prozent besitzen einen Breitbandzugang (Giannakouris und Smihily 2012). Mit 53 Prozent der Personen, die am Arbeitsplatz Internetdienste genutzt haben, liegen die Niederlande im EU-Vergleich mit den skandinavischen Ländern ganz vorne. Die mobile Breitbandnutzung ist bei Unternehmen in den Niederlanden allerdings nicht so ausgeprägt wie im Rest der EU. Nur 41 Prozent der Unternehmen stellten 2011 laut Eurostat ihren Beschäftigten ein tragbares Gerät mit mobilem Breitbandzugang zur Verfügung.

Niederländische Unternehmen sind laut einer Untersuchung überdurchschnittlich oft von Störungen ihrer IT-Systeme betroffen (Giannakouris und Smihily 2011). Während dies im EU-weiten Durchschnitt nur bei etwa 15 Prozent der Unternehmen der Fall ist, sehen sich in den Niederlanden 22 Prozent der Unternehmen mit Störungen konfrontiert. Bei diesen Störungen handelt es sich in 7 Prozent der Fälle um externe Angriffe auf die Webseite oder sonstige IKT-Dienste des Unternehmens. Damit weisen die Unternehmen in den Niederlanden, neben der Slowakei, den höchsten Anteil Störungen, die durch Cyberangriffe entstehen, innerhalb der Europäischen Union auf. Die häufigsten Auslöser für Störungen der IT-Systeme bei niederländischen Unternehmen sind laut der Untersuchung Probleme der Hard- oder Software (22 Prozent).

Trotz der hohen Zahl externer Angriffe liegen niederländische Unternehmen bei der Implementierung einer umfassenden Sicherheitspolitik laut Giannakouris und Smihily (2011) nur im europäischen Mittelfeld. Nur etwa 20 Prozent der Unternehmen weisen eine solche Sicherheitspolitik auf, die die wesentlichen Risiken der Informationssicherheit (Gefährdung durch Software- und Hardware-Probleme, Gefährdung durch Malware, Gefährdung durch externe Angriffe) adressiert. Deutlich besser schneiden niederländische Unternehmen ab, wenn es um Vorgaben zur Nutzung sicherer Passwörter (wird durch 53 Prozent der Unternehmen forciert) und die Nutzung von Hardware Tokens (zum Beispiel Smart Cards) für die sichere Authentifizierung, die von 17 Prozent der Unternehmen eingesetzt werden, geht. In beiden Fällen liegen die Werte über den EU-Durchschnittswerten.

Geringe Kenntnisse bezüglich der Gefahren, die durch die Internetnutzung entstehen können, und fehlendes technisches Wissen von Mitarbeitern wurden als wesentliche Gründe für mangelnde Informationssicherheit in niederländischen Unternehmen identifiziert (NCSC 2012). Darüber hinaus verweisen Giannakouris und Smihily (2011) darauf, dass niederländische Unternehmen generell deutlich weniger Aufwand, beispielsweise in Form von freiwilligen beziehungsweise verpflichtenden Fortbildungen oder sonstiger Informationsbereitstellung, im Kontext von Informationssicherheit betreiben, als dies im EU-Durchschnitt der Fall ist. Institutionen in den Niederlanden wie das CPNI.NL (2013) kritisieren, dass sich niederländische KMU zwar grundsätzlich sehr offen und interessiert für Empfehlungen und Verbesserungen zur Informationssicherheit zeigen, es jedoch häufig an der konkreten Umsetzung innerhalb der Unternehmen fehlt.

Im Juli 2013 wurde das dritte *Cyber Security Assessment Netherlands* (CSAN-3) veröffentlicht (NCSC 2013). Demnach sind niederländischen Unternehmen aktuell insbesondere der digitalen Spionage durch fremde Staaten und dem Diebstahl beziehungsweise der Manipulation von Informationen durch Kriminelle ausgesetzt.

5.3.3 Initiativen zur Informationssicherheit

Übergreifend ist das *Ministry of Security and Justice* in den Niederlanden für das Thema Cybersicherheit zuständig. Im Zuständigkeitsbereich des *Ministry of Security and Justice* wurde das nationale *Cyber Security Council* ins Leben gerufen, das sich aus Vertretern staatlicher, privater und wissenschaftlicher Organisationen zusammensetzt. Das *Cyber Security Council* ist sowohl für die Markt- und Trendbeobachtung im Bereich Cybersicherheit als auch für die Entwicklung übergreifender Sicherheitskonzepte zuständig.

Das zugehörige Exekutivorgan ist das im Jahr 2012 gegründete *National Cyber Security Center* (NCSC). Die Dienste des NCSC werden unter Federführung des *Ministry of Security and Justice* in Form einer öffentlich-privaten Kooperation zur Verfügung gestellt. Bislang sind nur staatliche Partner (zum Beispiel *Ministry of Economic Affairs, Agriculture and Innovation*,

Ministry of the Interior and Kingdom Relations, *Ministry of Foreign Affairs and Defense*, *Public Prosecution Service*, *General Intelligence and Security Service*, *National Police Services Agency*) involviert; in einem zweiten Schritt sollen dann auch privatwirtschaftliche Partner mit an Bord genommen werden. Die Aufgaben, der zuvor für die Themen Cybersicherheit und Krisenbewältigungsmaßnahmen, zuständigen Regierungsorganisation GOVCERT.NL, wurden vollständig ins NCSC überführt. Dem NCSC ist auch das *ICT Response Board* zuzuordnen, das im Krisenfall, das heißt einer nationalen Bedrohung durch Cyberangriffe, zusammentritt und Gegenmaßnahmen einleitet und koordiniert.

Unter Federführung des *Ministry of Security and Justice* und mit Beteiligung der zuvor genannten sowie einer Vielzahl weiterer Einrichtungen ist 2013 die zweite Auflage der *National Cyber Security Strategy* (NCSS2) für die Niederlande entstanden (Ministry of Security and Justice Netherlands 2013). Während die Erstauflage (2011) unter der Marschrichtung *From Ignorance to Awareness* stand (Ministry of Security and Justice Netherlands 2011), fokussiert die zweite Version auf den nun nächsten, notwendigen Schritt *From Awareness to Capability*. Die Strategie führt verschiedene Handlungsfelder auf, die in den nächsten zwei bis drei Jahren bearbeitet werden sollen. Hieraus abgeleitet werden auch eine Reihe geplanter Maßnahmen für diesen Zeitraum skizziert. Schwerpunkt ist hierbei der Schutz kritischer Infrastruktur sowie der Ausbau der Wissensbasis und Innovationsfähigkeiten im Bereich Cybersicherheit. Ein expliziter Fokus auf KMU ist bei den genannten Initiativen nicht erkennbar.

Eine laufende Initiative des NCSC mit Bezug auf KMU ist der *Waarschuwingsdienst*, der bereits vor einigen Jahren vom GOVCERT.NL gestartet und 2012 dann in den Verantwortungsbereich des NCSC übertragen wurde. Durch den *Waarschuwingsdienst* werden Bürger und Unternehmen, insbesondere KMU, die sich zuvor für den Dienst angemeldet haben, im Falle neuer Cyberbedrohungen per E-Mail oder SMS informiert. Aktuelle Entwicklungen werden darüber hinaus auf der Webseite der Initiative publiziert. Ende 2009 waren mehr als 65.000 Nutzer für den Benachrichtigungsdienst registriert; zusätzlich abonnierten mehr als 27.000 Nutzer den Newsletter der Initiative. Da sich der Fokus des NCSC laut eines Experteninterviews vom Schutz von KMU hin zum Schutz von Regierungsorganisationen und Institutionen verschoben hat, soll der *Waarschuwingsdienst* im Laufe des Jahres 2014 von einem neuen Dienst abgelöst werden.

Neben dem Justizministerium, das für die übergreifende, nationale Cybersicherheit verantwortlich zeichnet, gibt es mit Blick auf KMU zwei weitere zentrale Akteure in den Niederlanden. Hierbei handelt sich die *Koninklijke Vereniging MKB-Nederland* (MKB) sowie das *Digibewust*. Die MKB ist der Dachverband der niederländischen KMU. Ihm gehören verschiedene regionale und branchenspezifische Verbände an und er vertritt ungefähr 150.000 Unternehmen in den Niederlanden. *Digibewust* ist eine Partnerschaft aus Staat, Wirtschaft und Zivilgesellschaft, die sich der verantwortungsbewussten Nutzung des Internets verschrieben hat. Es wird vom niederländischen Wirtschaftsministerium, der Europäischen Kommission und verschiedenen Unternehmen unterstützt.

Gemeinsam mit dem Justizministerium haben die MKB und *Digibewust* im Dezember 2013 die Initiative *Hulpknop* (niederländisch für Notfallknopf) gestartet. Die Initiative richtet sich an Unternehmen, die Opfer eines Cyberangriffs geworden sind. Um den betroffenen Unternehmen eine Anlaufstelle zur Verfügung zu stellen, wurde eine zentrale Webseite aufgesetzt. Diese bietet Informationen wie Angriffe erkannt werden können und welche Gegenmaßnahmen jeweils ergriffen werden sollten. Die Informationen sind gegliedert nach vier Klassen von Angriffstypen: Internetbetrug (Malware, Phishing, Identitätsdiebstahl, Betrug), Verleumdung und üble Nachrede, Digitaler Einbruch (Industriespionage, Defacing, Passwörter

hacken) und Systemprobleme (Malware, DDoS-Angriffe). Neben Informationen wird auch eine zentrale Rufnummer der niederländischen Polizei bereitgestellt, unter der die Unternehmen Vorfälle melden und sich weitere Hilfe einholen können.

Aus demselben Kreis von Akteuren wird die Initiative *Cyberscan* betrieben. Hier werden KMU auf Basis von zehn Fragen sehr allgemein gehaltene Handlungsempfehlungen zur Verbesserung der Informationssicherheit zur Verfügung gestellt. Dazu werden verschiedene Dossiers rund um IT-Sicherheit angeboten, beispielsweise zu den Themen sichere Nutzung von E-Mails, Datenschutz, Internetbetrug.

Unter Finanzierung von *Digibewust* läuft auch die Initiative *Bescherm je bedrijf*, die von *Nederland ICT* betrieben wird. *Nederland ICT* ist der Branchenverband der 550 IKT-Unternehmen in den Niederlanden (Gesamtumsatz der Mitgliedsunternehmen 30 Milliarden Euro, 250.000 Mitarbeiter). Die Webseite *Bescherm je bedrijf* wurde im Jahr 2011 gestartet und ist als Initiative zur Bewusstseinsförderung angelegt. Nutzern der Webseite wird ein Quickscan zur Verfügung gestellt; dieser bietet ähnliche Funktionen und Aufbau wie der zuvor beschriebene Cyberscan. Darüber hinaus erhalten Nutzer ein individualisierbares, einfaches Planungswerkzeug zum Aufbau von Maßnahmen zur Cybersicherheit in der eigenen Organisation.

Die *Netherlands Organisation for Applied Scientific Research* (TNO) ist ein weiterer Akteur in den Niederlanden, der Initiativen zur IT-Sicherheit in KMU ins Leben gerufen hat. Die TNO ist eine Körperschaft öffentlichen Rechts und fokussiert auf angewandte Wissenschaft. Vergleichbar ist die TNO mit der deutschen Fraunhofer-Gesellschaft. Auftraggeber für Forschungsprojekte der TNO sind staatliche ebenso wie privatwirtschaftliche Organisationen. Das TNO betreibt ein Cyber Security Labor, das von innovativen Forschungsprojekten im Umfeld Cybersicherheit genutzt werden kann.

Gemeinsam mit dem MKB hat das TNO im März 2014 eine Konferenz zum Thema *Risiken der Cyberkriminalität* durchgeführt. Das MKB nutzte dabei sein landesweites Netzwerk, um Branchenvertreter und Experten zur Veranstaltung einzuladen. Zielgruppe der Veranstaltung waren Fachverbände verschiedener Branchen, die als Multiplikatoren das gewonnene Wissen an ihre Mitglieder weitergeben sollen. Im Rahmen der Konferenz wurde auch eine zweite Initiative der TNO vorgestellt: das *Cyberrad*. Das *Cyberrad* ist ein Werkzeug das auf KMU zugeschnitten ist. KMU können das Online-Tool nutzen, um für die eigene Branche typische Angreifer- und Angriffsprofile zu ermitteln und Hilfestellung für entsprechende Präventiv- beziehungsweise Gegenmaßnahmen zu erhalten. Das Cyberrad wird ebenfalls im Zuge der Website www.stopcybercrime.nu verbreitet.

Der niederländische Geheimdienst stellt Unternehmen seine Erkenntnisse über Cyberbedrohungen und aktuell laufende Cyberangriffe zur Verfügung. Das dies geschieht ist dem jährlich veröffentlichten Bericht zu entnehmen (AIVD 2013). In welchem Rahmen und in welcher Form dieser Dienst angeboten wird, konnte im Rahmen der Recherche für dieses Projekt nicht geklärt werden. Es waren keine öffentlich zugänglichen Unterlagen identifizierbar; auch in den Experteninterviews konnten hierüber keine Erkenntnisse gesammelt werden.

Zum Thema Cybersicherheit wurden mehrere nationale Forschungsprogramme in den Niederlanden aufgesetzt. Unter dem Dach des *Rijksdienst voor Ondernemend Nederland* (RVO) werden momentan im Rahmen von *Small Business Innovation Research* (SBIR) zwei Förderprogramme zum Thema durchgeführt. Im ersten Programm wurden, im Zeitraum September 2012 – Dezember 2014, 14 Machbarkeitsstudien durchgeführt. Zu acht dieser

Projekte wurden beziehungsweise werden im Anschluss Prototypen entwickeln. Für das zweite Programm (Mai 2014 – Juli 2016) läuft zum Zeitpunkt der vorliegenden Untersuchung die Ausschreibung für die Finanzierung weiterer 20 Machbarkeitsstudien. Im Abschluss befindet sich das Programm *Sentinels*, das 2004 gestartet wurde und in drei Phasen 16 Forschungsprojekte zum Thema IKT-Sicherheit finanziert hat (NWO 2011). Die Projekte wurden in enger Zusammenarbeit zwischen Forschungsinstitutionen und Industrieunternehmen durchgeführt. Der Fokus der Projekte lag auf der Entwicklung technischer Lösungen.

5.3.4 Wesentliche Erkennnisse

Die Niederlande sind eine sehr IT-affine Gesellschaft. Der Schwerpunkt bei den niederländischen Initiativen zur Förderung der Informationssicherheit liegt im Bereich der Mittelstandspolitik. Dementsprechend sind hier vor allem wirtschaftsnahe Einrichtungen involviert. Bei den Initiativen ist zu beobachten, dass diese eher langfristig angelegt und auch Forschungseinrichtungen durch sogenannte R&D-Programme eingebunden sind. In den Niederlanden sind mit dem MKB oder auch *Nederland ICT* mehrere Unternehmensverbände prominent in der Förderung der Informationssicherheit vertreten.

5.4 Österreich

5.4.1 Kurzüberblick

Struktur der kleinen und mittelständischen Unternehmen

Mittlere Unternehmen	4.897	491.152	33 Mrd. €
Kleinunternehmen	32.250	619.981	31 Mrd. €
Kleinstunternehmen	263.585	659.975	29 Mrd. €
Summe	**300.732**	**1.771.108**	**93 Mrd. €**
Anteil an Gesamtwirtschaft	99,7 Prozent	67,7 Prozent	60,1 Prozent

Quelle: Europäische Kommission (2013c)

Bedeutung und Stand der Informationssicherheit

- Österreichische Unternehmen nutzen sowohl überdurchschnittlich häufig feste als auch mobile Breitbandverbindungen
- Obwohl KMU in hohem Maße von ihrer IT abhängig sind, verfügen mehr als 30 Prozent über keinerlei Notfallplan

Wesentliche Akteure und Initiativen

- Sowohl verschiedene Bundesministerium als auch das Bundeskanzleramt sind sehr aktiv
- Vom Bundeskanzleramt wurde die Nationale *IKT-Sicherheits-Strategie* herausgegeben und als Ergänzung die *Österreichische Strategie für Cyber Sicherheit*
- Die *Wirtschaftskammer Österreich* (WKO), die maßgeblich Maßnahmen zur Stärkung der Informationssicherheit in KMU initiiert
- Das *Kuratorium Sicheres Österreich* (KSÖ) wurde zur besseren Abstimmung zwischen der Wirtschaft und staatlichen Behörden gegründet

5.4.2 Bedeutung und Stand der Informationssicherheit

Rund drei Viertel der Österreicher nutzt mittlerweile regelmäßig das Internet, mehr als 60 Prozent bereits täglich (Eurostat 18.12.2013). Durch die hohe Nutzungsrate von Sicherheitssoftware (87 Prozent) lag 2011 die Rate der infizierten Rechner in Österreich bei sehr niedrigen 14 Prozent (Eurostat 08.02.2011).

Die Rate der Unternehmen mit Internetzugang liegt im Jahr 2012 mit 98 Prozent noch über dem schon hohen EU27-Durchschnitt von 95 Prozent (Giannakouris und Smihily 2012). Während die Ausstattung mit festen Breitbandverbindungen mit 82 Prozent im Vergleich nicht sonderlich hoch ausgeprägt ist, liegt die Quote der von Unternehmen genutzten mobilen Breitbandverbindungen mit 58 Prozent deutlich über dem EU-Schnitt (48 Prozent). Dies ist sicherlich auch mit den geographischen Gegebenheiten in Österreich, zum Beispiel wenig Ballungsgebiete, zu erklären. Ein deutlicher Unterschied ist hier zwischen kleinen Unternehmen (53 Prozent) und mittleren Unternehmen (83 Prozent) zu erkennen.

Bei einer Studie von Reisinger (2013), die im Rahmen einer Bachelorarbeit durchgeführt wurde, gaben mehr als 80 Prozent der befragten österreichischen Unternehmen an, in ihren Kerngeschäftsprozessen und -tätigkeiten (sehr) stark von der Funktionalität ihrer IT-Systeme abhängig zu sein. Diese Aussage wird gestützt durch eine Befragung der Unternehmensberatung KPMG (2004), bei der ebenfalls 80 Prozent der befragten Unternehmen ihre IT-Abhängigkeit als sehr hoch einschätzten. Durch die hohe Abhängigkeit von IKT, muss bei einem Ausfall mit erheblichen finanziellen und zeitlichen Einbußen gerechnet werden. Teilweise könnte der Betrieb sogar vollständig zum Erliegen kommen. In der Befragung gaben immerhin 56 Prozent der Unternehmen an, dass es zu einer erheblichen Geschäftsunterbrechung kommen würde, wenn auf wesentliche Unternehmensdaten nicht mehr zugegriffen werden könnte.

KMU in Österreich sehen sich mit einer Vielzahl von IT-Sicherheitsproblemen konfrontiert. Im Jahr 2010 wurden 9 Prozent (kleine Unternehmen) bzw. 13 Prozent (mittlere Unternehmen) Opfer eines IKT-bezogenen Sicherheitsvorfalles. Laut einer Untersuchung von Cisco Austria (2012) sind sogar 42 Prozent aller Unternehmen von Systemausfällen durch Schadsoftware betroffen. Die österreichische Kriminalitätsstatistik weist einen leichten Rückgang der Kriminalität insgesamt aus, die Anzahl erfasster Fälle von Cyberkriminalität nahm im gleichen Zeitraum jedoch zu (Bundesministerium für Inneres Österreich (2013)). Nachdem sich die Fallzahlen von 2012 nach 2013 mehr als verdoppelten, gab es von 2013 nach 2014 immer noch einen Anstieg von 8,6 Prozent. Häufigster Fall ist Internetbetrug (68 Prozent der Fälle). Das CERT.at verzeichnete 2012 rund 12.900 Berichte, von denen knapp ein Drittel als ernstzunehmende Sicherheitsvorfälle einzuordnen sind (CERT.at 2013). Anfang 2013 wurde ein massiver Anstieg von Fällen gezielten Manipulierens von Webseiten (sogenanntes *Website-Defacements*) in Österreich beobachtet – teilweise mehr als 1.000 Vorfälle im Monat. Die Untersuchung von Reisinger (2013) identifiziert Malware, Hardware oder Softwarefehler, Stromausfälle und Phishing als häufigste Ursachen für IT-Sicherheitsprobleme, Störungen und Schäden in österreichischen KMU. Eine Befragung von Unternehmen durch KPMG ergibt, dass 81 Prozent der Unternehmen in Österreich, die schon von Cyberkriminalität betroffen waren, mobile Datenträger als risikobehaftet ansehen (Geschonneck und Fritzsche 2013). 73 Prozent nennen in diesem Zusammenhang mobile Telekommunikation als Risikofaktor. Diese Wahrnehmung stimmt auch mit den gemeldeten Fällen von Cyberkriminalität überein – Smartphones werden in Österreich viermal häufiger das Ziel von Angriffen als in Deutschland.

Durch die beschriebene, hohe IT-Abhängigkeit der Unternehmen muss bei Systemausfällen mit erheblichen finanziellen und zeitlichen Einbußen gerechnet werden. Teilweise kann der Geschäftsbetrieb sogar gänzlich zum Erliegen kommen (Kurki 2006). Fälle von Cyberkriminalität richten im Durchschnitt einen Schaden in Höhe von 400.000 Euro an, in Einzelfälle werden Schadenssummen in Millionenhöhe erreicht – zu dieser Erkenntnis kommt eine Untersuchung durch den Verband der Versicherungsunternehmen Österreichs (VVO) (24.04.2014). Von mehr als 40 Prozent der Unternehmen, die in einer Studie von Cisco Austria (2012) befragt wurden, wird der potentielle Schaden als hoch bzw. sogar existenz-

bedrohend eingeschätzt. Diese Studie sieht einen großen Nachholbedarf bei der IT-Sicherheit in österreichischen Unternehmen. So geben zwar 96 Prozent der Führungskräfte an, dass ihnen die Sicherheitsbedrohungen bekannt sind, aber 38 Prozent wissen nur wenig oder gar nichts darüber, ob ihr Unternehmen ausreichend geschützt ist. Diese Wahrnehmung wird auch von Studien der TU Wien und Universität Wien (TU Wien 18.02.2013) und der WKO (Computerwelt.at 03.03.2014) gestützt. Laut der WKO-Studie erwarten mehr als die Hälfte der befragten Einpersonenunternehmen (53,7 Prozent) gar keinen oder nur einen geringen Schaden durch eine Cyberattacke, bei den Großunternehmen sind hingegen nur 17,2 Prozent dieser Auffassung. Unter den IT-Sicherheitsproblemen führen in dieser Befragung IT-Systemausfälle (31,1 Prozent), Probleme mit Spam (30,9 Prozent), Virenangriffe (28,7 Prozent), Datenverlust (17,2 Prozent) und Verlust oder Diebstahl mobiler Geräte (16,8 Prozent) die Rangliste an. Auch Geschonneck und Fritzsche (2013) kommen in ihrer Untersuchung zu einer ähnlichen Erkenntnis. Hier gibt mehr als ein Drittel der betroffenen Unternehmen an, dass sie durch Zufall auf Sicherheitsvorfälle aufmerksam geworden sind. Darüber hinaus nennen 96 Prozent der Unternehmen mangelnde Sicherheitskultur als großen Risikofaktor.

Eine Studie zeigt, dass trotz der zuvor beschriebenen Relevanz der IT für KMU mehr als 30 Prozent der Unternehmen über keinerlei Notfallpläne für ihre IT verfügen (Reisinger 2013). Demgegenüber stehen etwa 42 Prozent der Unternehmen, die adäquate Notfallpläne für den Ausfall ihrer IKT-Systeme definiert und implementiert haben. Diese Zahlen werden auch durch die zuvor erwähnte Studie der WKO gestützt (Computerwelt.at 03.03.2014). Demnach haben 75 Prozent der Einpersonenunternehmen und mehr als die Hälfte der Kleinstunternehmen keine derartigen Pläne vorliegen. Reisinger (2013) untersucht auch den Stand und Einsatz technischer Maßnahmen zum Schutz der Informationssicherheit in KMU. Hierbei zeigt sich, dass nur etwa 30 Prozent der KMU Firewalls, Viren-Scanner, Malware-Scanner und Backup-Software einsetzen. Technologien für sichere Authentifizierungsvorgänge werden sogar nur von lediglich 15 Prozent der befragten Unternehmen genutzt und nur weitere 2 Prozent planen die Implementierung solcher Technologien. Insgesamt geben über 40 Prozent der Unternehmen an, keine speziellen Standards im Bereich der Informationssicherheit zu verwenden. Dies ist darauf zurückzuführen, dass aufwendigere Sicherheitsmaßnahmen mit höheren Kosten verbunden sind. Eben diese Kosten sind einer der ausschlaggebenden Gründe für den fehlenden Einsatz von umfangreichen Informationssicherheitsmaßnahmen (Kurki 2006).

Kurki (2006) identifiziert in seiner Studie mangelndes Wissen oder Bewusstsein, hohe Kosten und Zeitaufwand als Hauptgründe für mangelnde Maßnahmen zur Informationssicherheit. Außerdem wird jedoch festgestellt, dass sich KMU deutlich objektivere Informationen und Tests zu bestehenden Sicherheitsmaßnahmen wünschen. Dabei wäre ein System im Sinne der Verbraucherorganisation Stiftung Warentest wünschenswert. Der Fokus sollte auf Sicherheitslösungen für KMU gelegt werden, die dann von staatlicher Seite bewertet würden.

5.4.3 Initiativen zur Unterstützung von Informationssicherheit

Die *Nationale IKT-Sicherheits-Strategie Österreich* gibt die übergeordnete, nationale Ausrichtung zum Thema Informationssicherheit in Österreich vor (Bundeskanzleramt Österreich 2012). Das wesentliche Ziel der Strategie ist der Schutz der kritischen Infrastrukturen. Darüber hinaus wird jedoch auch ein besonderes Augenmerk auf den Schutz und den Ausbau des Sicherheitsniveaus bei KMU gelegt. Herausgeben wurde die nationale Strategie durch das *Bundeskanzleramt* Österreich unter Mitarbeit verschiedener privatwirtschaftlicher und staatlicher Institutionen. Das Bundeskanzleramt ist einer der zentralen staatlichen

Akteure beim Thema Informationssicherheit auf nationaler Ebene in Österreich. In Kooperation mit dem CERT.at betreibt es seit 2008 das GovCERT, das die Verhinderung bzw. Behandlung von IKT-Sicherheitsvorfällen innerhalb der Regierungsnetze und -systeme zur Aufgabe hat. Darüber hinaus koordiniert das Bundeskanzleramt den Schutz kritischer Infrastrukturen in Österreich.

Als eine der ersten Initiativen ist das Portal *onlinesicherheit.gv.at* aus der nationalen Strategie hervorgegangen. Auftraggeber und Betreiber des Portals sind neben dem *Bundeskanzleramt*, das *Bundesministerium für Finanzen* und das *Zentrum für sichere Informationstechnologie – Austria* (A-SIT). Das Portal stellt Informationen für verschiedene Zielgruppen zur Verfügung, insbesondere werden hier Unternehmen und ihre Mitarbeiter angesprochen. Über das Portal kann u.a. das *Österreichische Informationssicherheitshandbuch* (SIHA) kostenlos heruntergeladen werden (Bundeskanzleramt Österreich (2013b)). Das Handbuch unterstützt Unternehmen und Organisationen der öffentlichen Verwaltung beim Aufbau und der Einführung eines umfassenden ISMS. Mit der Überarbeitung im Jahr 2010 wurde das SIHA auf die Umsetzung von ISM-Maßnahmen (z.B. ISO/IEC 27000 Normenreihe) in KMU zugeschnitten (Bundeskanzleramt Österreich 2012). Dabei wurde auf die Erfahrungen des BSI und des schweizerischen *Informatikstrategieorgan des Bundes* (ISB) zurückgegriffen.

Neben dem Bundeskanzleramt sind das *Bundesministerium für Inneres*, das *Bundesministerium für Landesverteidigung und Sport* sowie das *Bundesministerium für europäische und internationale Angelegenheiten* wesentliche staatliche Akteure im Umfeld Informationssicherheit in Österreich. Im Jahr 2013 wurde durch diese Organisationen, als Ergänzung zur *Nationalen IKT-Sicherheits-Strategie Österreich*, die *Österreichische Strategie für Cyber Sicherheit* (ÖSCS) veröffentlicht (Bundeskanzleramt Österreich 2013a). Die ÖSCS bildet die Grundlage für die gesamtstaatliche Zusammenarbeit zum Schutz des Cyberspace. Dazu wird auf nationaler Ebene eine Struktur zur Koordination und für einen regelmäßigen Informationsaustausch definiert. Das CERT.at übernimmt hierbei die zentrale Anlaufstelle bei Sicherheitsvorfällen – über die eingerichteten *Austrian Trust Circles* vernetzen sich Sicherheitsexperten der Branchen, die kritische Infrastrukturen betreiben.

Maßnahmen zur Steigerung der Informationssicherheit in KMU werden vor allem durch die *Wirtschaftskammer Österreich* (WKO) initiiert. Die WKO, eine Körperschaft öffentlichen Rechts, koordiniert übergreifend die Aktivitäten der Wirtschaftskammern der Bundesländer. Die Landeskammern sind die Interessensvertretungen aller gewerblich tätigen Wirtschaftstreibenden. Es besteht eine gesetzlich verpflichtende Mitgliedschaft (ca. 450.000 Mitgliedsunternehmen). Innerhalb des Fachverbands *Unternehmensberatung, Buchhaltung und Informationstechnologie* (UBIT) der WKO wurde die *IT-Security Experts Group* eingerichtet. Ziel dieser Expertengruppe ist die Verbesserung der Informations- und IT-Sicherheit in KMU und die Positionierung von IT-Security Spezialisten als zentrale Ansprechpartner für Unternehmen bei Fragen zur IT-Sicherheit. Finanziert durch das *Bundesministerium für Wissenschaft, Forschung und Wirtschaft* hat die *IT-Security Experts Group* in den Jahren 2006-2007 Sicherheitschecks in KMU im Umfang eines halben Personentages durchgeführt. Dazu wurden im Vorfeld – auf verschiedenen Veranstaltungen –Gutscheine an Unternehmen verteilt, die diese für den Sicherheitscheck einlösen konnten.

Eine weitere Initiative der WKO ist die Webseite *it-safe.at*. Über diese Plattform wird KMU-spezifisches Informationsmaterial bereitgestellt. Neben allgemeinen Informationen zu Informationssicherheit steht KMU ein Risikoanalysetool zur Verfügung, über das innerhalb kürzester Zeit ein erstes Risikoprofil des eigenen Unternehmens erstellt werden kann. Entsprechend des Risikoprofils werden Maßnahmen zur Verbesserung der Informationssi-

cherheit aufgeführt. Weiterhin stehen auf der Webseite zwei Handbücher zur IT-Sicherheit für KMU[26] zum kostenlosen Download. Die Handbücher adressieren unterschiedliche Zielgruppen innerhalb von KMU: a) Geschäftsführung und b) Mitarbeiter. Die gedruckten Versionen der Handbücher wurden bereits mehr als 50.000 Mal angefordert. Nicht verwechselt werden sollten das SIHA sowie die hier angeführten IT-Sicherheitshandbücher für KMU.

WKO und CERT.at eruieren aktuell die Möglichkeiten für die Bereitstellung eines Meldedienstes für KMU. Hierzu sollen Meldungen über IT-Sicherheitsbedrohungen zielgruppengerecht gefiltert und aufbereitet werden. Weitere Informationen zu diesem Vorhaben waren zum Zeitpunkt der Recherche nicht verfügbar.

Die Initiative *Sicher im Internet* wurde 2005 von Microsoft initiiert und seitdem auch operativ betrieben. Neben dem *Bundesministerium für Inneres* und der WKÖ unterstützen eine Reihe anderer Organisationen und Unternehmen die Initiative. Auf der Website von *Sicher im Int*ernet werden KMU kostenlos Checklisten angeboten, mit deren Hilfe sie ihren IT-Sicherheitsstand überprüfen und gegebenenfalls verbessern können.

Zur besseren Abstimmung zwischen der Privatwirtschaft und den staatlichen Behörden wurde das *Cyber-Security Forum* des *Kuratoriums Sicheres Österreich* (KSÖ) ins Leben gerufen (Der Standard 2013). Das Forum soll einen besseren Schutz von KMU vor Cyberangriffen ermöglichen. Das KSÖ ist ein unabhängiger Verein (Partnerorganisation des *Bundesministerium für Inneres* und der österreichischen Bundespolizei), der sich als nationale Vernetzungs- und Informationsplattform im Bereich innere Sicherheit versteht. Das Thema Cybersicherheit nimmt in der Arbeit des Vereins einen zunehmend höheren Stellenwert ein. Zwei der vier Schwerpunkte des KSÖ (Cyber Security und Cyber Crime) beschäftigen sich mit diesem Themenkomplex. Das KSÖ führte in Zusammenarbeit mit der WKO und dem *Bundesministerium für Inneres* 2013 erstmals die Roadshow *Schutz vor Cyberkriminalität* durch. Hier informierten Sicherheitsexperten KMU über mögliche Gefahren im Zusammenhang mit der Nutzung des Internets.

2005 startete Österreich mit KIRAS als einer der ersten europäischen Staaten ein nationales Sicherheitsforschungsprogramm mit zivilem Fokus. Langfristig sollen die durch KIRAS geförderten Projekte dazu beitragen, qualifizierte Arbeitsplätze in Österreich zu schaffen und einen Beitrag zur österreichischen Wertschöpfung zu leisten. Die Programmverantwortung liegt beim *Bundesministerium für Verkehr, Innovation und Technologie*; das Budget der ersten Programmphase (2005-2013) wurde mit 60 Millionen Euro veranschlagt. Bis heute wurden rund 100 Projekte gefördert. Voraussichtlich im Oktober 2014 findet die nächste Ausschreibungsphase statt.

5.4.4 Wesentliche Erkenntnisse

In Österreich sind an den Initiativen zum Thema Informationssicherheit, ähnlich wie in Deutschland, nationale Regierungsbehörden in erheblichem Umfang beteiligt. Maßgeblich in Österreich sind hier neben dem *Bundeskanzleramt* das *Bundesministerium für Inneres*, *das Bundesministerium für Landesverteidigung und* Sport sowie das *Bundesministerium für europäische und internationale Angelegenheiten*. Darüber hinaus sind mit dem WKO als Unternehmensverband und dem KSÖ als Koordinationsorgan zwischen staatlichen und privatwirtschaftlichen Partnern weitere Akteure vertreten. Der Fokus der Initiativen liegt in der Mittelstandsförderung. Das IT-Sicherheitshandbuch für KMU besitzt mit 50.000

[26] Vgl. WKÖ (2014a) sowie WKÖ (2014b).

angeforderten Printexemplaren – ohne die Downloads zu zählen – eine sehr große Reichweite.

5.5 Schweden

5.5.1 Kurzüberblick

Struktur der kleinen und mittelständischen Unternehmen

Mittlere Unternehmen	4.615	518.414	31 Mrd. €
Kleinunternehmen	27.354	623.452	32 Mrd. €
Kleinstunternehmen	599.821	772.944	39 Mrd. €
Summe	**631.790**	**1.914.809**	**101 Mrd. €**
Anteil an Gesamtwirtschaft	99,8 Prozent	64,8 Prozent	57,4 Prozent

Quelle: Europäische Kommission (2013f)

Bedeutung und Stand der Informationssicherheit

- Sowohl bei Privatpersonen als auch bei Unternehmen liegt die Internetnutzung über dem EU-Durchschnitt
- Nahezu jedes zweite schwedische Unternehmen verfügt über eine formal definierte IKT-Sicherheitspolitik

Wesentliche Akteure und Initiativen

- Die *Swedish Civil Contingencies Agency* (MSB) gehört zum Verteidigungsministerium und übernimmt aktuell das Mandat KMU über Informationssicherheit zu informieren.
- Die *Post and Telecom Authority* (PTS) verliert gerade ihre Kompetenzen an die MSB
- Insgesamt liegt der Fokus in Schweden auf dem Schutz der kritischen Infrastruktur und es gibt nur wenige Initiativen die KMU adressieren

5.5.2 Bedeutung und Stand der Informationssicherheit

In Schweden besitzen bereits 93 Prozent der Haushalte einen Internetanschluss. 92 Prozent der Schweden nutzen regelmäßig das Internet, 81 Prozent davon sogar täglich, was weit über dem EU-Durchschnitt von 72 bzw. 62 Prozent liegt (Eurostat 18.12.2013). Um sich und ihren Computer zu schützen, verwenden 89 Prozent der Schweden eine Antivirensoftware. Dennoch sind 31 Prozent der Rechner dort infiziert (Eurostat 08.02.2011).

Von den 98 Prozent der schwedischen Unternehmen, die 2012 über einen Internetanschluss verfügten (EU-Durchschnitt 95 Prozent) hatten 95 Prozent einen Breitbandanschluss, was ebenfalls über dem EU-Durchschnitt von 90 Prozent lag (Giannakouris und Smihily 2012). Eine mobile Breitbandverbindung wurde von 63 Prozent der schwedischen Unternehmen genutzt, was den EU-Durchschnitt von 48 Prozent bei weitem übertraf. Dabei unterschieden sich kleine Unternehmen mit 59 Prozent erheblich von mittleren Unternehmen, von denen schon 85 Prozent mobile Breitbandverbindungen verwendeten.

Laut einer detaillierten Analyse der Störungen von IKT-Systemen bei Unternehmen in den Mitgliedsstaaten der Europäischen Union, werden schwedische Unternehmen häufiger mit Störungen konfrontiert (19 Prozent) als dies im Durchschnitt bei Unternehmen in anderen europäischen Mitgliedstaaten der Fall ist (15 Prozent) (Giannakouris und Smihily 2011).

Bei 16 Prozent der schwedischen Unternehmen stellen Störungen von Hard- und Software die häufigste Ursache der Störungen von IKT-Systemen dar, während 4 Prozent der Unternehmen Ausfälle auf Grund von externen Angriffen zu verzeichnen haben. 2 Prozent der Unternehmen sind von Viren oder Malware betroffen, die nicht-autorisierten Zugang zu

den Systemen ermöglichen. Von Phishing und Pharming sind lediglich unter 1 Prozent der schwedischen Unternehmen betroffen (Giannakouris und Smihily 2011).

Nach dem aktuellen Stand der Recherche lässt sich festhalten, dass 46 Prozent der schwedischen Unternehmen über eine formal definierte IKT-Sicherheitspolitik verfügen. Dieser Wert liegt deutlich über dem europäischen Durchschnitt von 26 Prozent. Außerdem sind sich 82 Prozent der Unternehmen möglicher Gefahren der Internetnutzung bewusst und setzen entsprechende Sicherheitssoftware oder -Tools ein, um ihre Systeme effektiv vor diesen Gefahren zu schützen. Der Wert liegt ebenfalls deutlich über dem Durchschnittswert der europäischen KMU, in Höhe von 59 Prozent (ENISA 2011c).

Als Hauptursache für mangende Informationssicherheit führen die Jahresberichte der *Swedish Civil Contingencies Agency* (MSB) zwischen den Jahren 2005 und 2011 mangelnde technische Kenntnisse an, während die *Swedish Post and Telecom Authority* (PTS) fehlendes Problembewusstsein im Umgang mit Informationstechnik bemängeln (PTS 2005). Eine weitere Ursache ist das bisherige Fehlen eines einheitlichen Systems zur Meldung von Vorfällen (Incident Reporting) auf Seiten des schwedischen Staates. Durch diesen Mangel gehen wichtige Informationen zu Angriffen in KMU verloren, die weiteren Angriffen vorbeugen könnten und die Vorkehrungen in KMU verbessern könnten (PTS 2006).

5.5.3 Initiativen zur Informationssicherheit

Im Gegensatz zu vielen anderen europäischen Ländern verfügt Schweden über keine übergeordnete Cybersicherheitsstrategie. Dennoch existieren einige Institutionen, die sich mit dem Thema Informationssicherheit beschäftigen. Wie sowohl die Literaturrecherche als auch das Führen von Experteninterviews ergeben haben, existieren wenige Initiativen die einen speziellen Schwerpunkt auf KMU legen.

Einer der maßgeblichen Akteure im Bereich Informationssicherheit in Schweden ist die *Swedish Civil Contingencies Agency* (MSB), die sich um das nationale Krisenmanagement kümmert und direkt dem Verteidigungsministerium unterstellt ist. Die MSB hat bisher zwei Nationale Cybersicherheitsübungen (NISÖ) durchgeführt, die auf die kritische Infrastruktur abzielten. Aus Sicht der MSB zählen hierzu durchaus auch KMU.

Insgesamt verschieben sich die Kompetenzen bezüglich Informationssicherheit in Schweden zusehends von der *Swedish Post and Telecom Authority* (PTS), die zum *Ministry of Enterprise, Energy and Communications* gehört, hin zur MSB und damit zum Verteidigungsministerium. Auf diese Weise übernahm die MSB auch den Betrieb des *SE-CERT*, das zuvor von der PTS unterhalten wurde.

Ein weiterer Indikator sind Planungen der MSB ein umfangreiches Informationsangebot zu Informationssicherheit für KMU aufzulegen, das als Nachfolger für ein ähnliches Programm der PTS gesehen werden kann. Dabei plant die MSB auf bestehende Angebote aufzubauen. Momentan befinden sich auf der Website der PTS Informationen zu einer großen Bandbreite von möglichen Bedrohungen der IT-Sicherheit und Maßnahmen, sich vor denselben zu schützen. Das entsprechende Mandat durch die schwedische Regierung KMU über IT-Sicherheit aufzuklären hatte die PTS seit 2005 inne, doch mit diesem Jahr geht das Mandat an die MSB über.

Von der PTS wurde von 2007-2008 darüber hinaus in Kooperation mit Großunternehmen aus dem IT-Sektor wie Microsoft und Symantec eine *Info-Tour* durchgeführt. Obwohl diese Veranstaltungen zunächst für die allgemeine Öffentlichkeit gedacht waren, verschob sich der

Fokus schnell auf KMU. Pro Jahre wurden im Frühjahr und Herbst je Vier Veranstaltungen in schwedischen Städten durchgeführt. Da die Informationsveranstaltungen jedoch keinen messbaren Erfolg brachten, wurden sie bereits nach dem 2. Jahr wieder eingestellt.

Neben den beiden staatlichen Behörden MSB und PTS, sind im akademischen Bereich weitere Akteure und Initiativen zu finden. Das *Royal Institute of Technology* (KTH), die Königliche Technische Hochschule in Stockholm, führt bereits seit 1996 Kurse und Seminare zur Cybersicherheit durch, die auch KMU offen stehen. Auf diese Weise erhalten speziell KMU ohne eigene IT-Abteilung Zugang zu akademischer Expertise zum Thema.

Neben dieser Initiative der KTH engagieren sich weitere akademische Institutionen im Bereich Informationssicherheit, die sich aus Instituten mehrerer schwedischer Universitäten zusammensetzen (ENISA 2011c). Durch dieses Netzwerk wurde unter Leitung der MSB ein Maßnahmenkatalog definiert, um die Informationssicherheit weiter zu verbessern (MSB 2011). Der Katalog umfasst Maßnahmen zu den Themen: Operative Sicherheit, Praktikabilität, Zugangsmöglichkeiten, Authentifizierung, Veränderungsschutz und, sofern notwendig, Geheimhaltung (PTS 2005).

Das Projekt ISIS (IT-Sicherheit in Skandinavien) ist ein norwegisch-schwedisches Gemeinschaftsprojekt mit dem seit dem 1. Januar 2013 versucht wird, die Kooperation zwischen Hochschulen, Behörden und Unternehmen in den beiden Ländern im Bereich IT-Sicherheit zu verbessern. Auf schwedischer Seite ist die *Compare Karlstadt Stiftung* federführend, der mehr als 100 Unternehmen, die *Karlstadt Universität* sowie weitere öffentliche Einrichtungen angehören. Es werden Seminare, Workshops und Konferenzen zu einer großen Bandbreite von Themen (u.a. *Internet und Sicherheit* oder *Security Divas*, einer Konferenz für Frauen) angeboten.

5.5.4 Wesentliche Erkenntnisse

Schweden verfolgt bei seinen Initiativen zur Förderung der Informationssicherheit in KMU neben geostrategischen Zielen ebenfalls eine klassische Mittelstandsförderung, wobei allerdings momentan eine Verschiebung der Kompetenzen für den Schutz von KMU vor Bedrohungen der Informationssicherheit vom *Ministry of Enterprise, Energy and Communications* zum Verteidigungsministerium stattfindet. Zu erwähnen ist noch der bilaterale Ansatz, den Schweden und Norwegen mit ihrer Initiative Isis (IT-Sicherheit in Skandinavien) verfolgen.

5.6 Spanien

5.6.1 Kurzüberblick

Struktur der kleinen und mittelständischen Unternehmen

Mittlere Unternehmen	15.484	1.513.350	73 Mrd. €
Kleinunternehmen	120.940	2.297.597	91 Mrd. €
Kleinstunternehmen	2.103.390	4.318.258	121 Mrd. €
Summe	**2.239.814**	**8.129.205**	**284 Mrd. €**
Anteil an Gesamtwirtschaft	99,9 Prozent	74,9 Prozent	64,8 Prozent

Quelle: Europäische Kommission (2013a)

Bedeutung und Stand der Informationssicherheit

- Während Haushalte in Spanien mit der Internetnutzung unter dem EU-Durchschnitt liegen, verfügen spanische Unternehmen überdurchschnittlich oft über einen Internetzugang
- Spanische KMU sehen den Mangel an auf ihre Bedürfnisse zugeschnittenen Produkten und Dienstleistungen als problematisch an

Wesentliche Akteure und Initiativen

- *Instituto Nacional de Tecnologías de la Comunicación* (INTECO) ist die zentrale staatliche Institution im Bereich Informationssicherheit, die das *INTECO-CERT sowie* verschiedene weitere Programme unterhält
- Das *Industrial Cyber Security Center* (CCI) thematisiert Cybersicherheit in Spanien und Lateinamerika und kümmert sich speziell um den Mangel an spanischsprachigen Dokumenten zum Thema

5.6.2 Bedeutung und Stand der Informationssicherheit

In Spanien besitzen lediglich 70 Prozent der Haushalte einen Internetanschluss, was wesentlich unter dem EU-Durchschnitt von 79 Prozent liegt Regelmäßig wird das Internet in Spanien von 66 Prozent der Bevölkerung genutzt, von 54 Prozent sogar täglich (Eurostat 18.12.2013). Die Nutzung einer IT-Sicherheitssoftware lag 2011 mit 84 Prozent genau im EU-Durchschnitt, wobei die Zahl der infizierten Rechner mit 33 Prozent leicht darüber lag (Eurostat 08.02.2011).

Auf Unternehmensseite verfügten 97 Prozent 2012 über einen Internetzugang und 95 Prozent über eine Breitbandverbindung, was beides über den EU Durchschnittswerten von 95 respektive 90 Prozent lag. Die von Unternehmen genutzten mobilen Breitbandverbindungen lagen mit 45 Prozent leicht unter dem EU-Durchschnitt von 48 Prozent, wobei auch in Spanien eine starke Differenzierung zwischen kleinen Unternehmen mit 41 Prozent und mittleren Unternehmen mit 71 Prozent zu beobachten war (Giannakouris und Smihily 2012).

Viele spanische KMU sehen sich mit Angriffen und Störungen ihrer Informationssicherheit konfrontiert, die zum Teil erhebliche Behinderungen der Unternehmenstätigkeiten nach sich ziehen. Faktisch dokumentiert dies eine, durch das *Instituto Nacional de Tecnologías de la Comunicación* (INTECO) veröffentlichte, Studie, in der eines von drei Unternehmen sich im Jahr 2011 mit IT-Sicherheitsproblemen auseinandersetzen musste, die die reguläre Fortführung des Betriebs gefährdeten (INTECO 2012b). Einen weiteren Beleg für die akute Bedrohung der Informationssicherheit liefert eine Untersuchung bei Unternehmen mit bis zu 49 Angestellten, in der sich herausstellte, dass knapp 50 Prozent der untersuchten Rechner mit Malware, vornehmlich Trojanern, infiziert waren (INTECO 2010).

Häufigste Ursachen für Störungen der Informationssicherheit in den lokalen IT-Systemen der Unternehmen sind Malware, Spam und technisches Versagen (INTECO 2012a). Hingegen

entstehen die Informationssicherheit gefährdende Vorkommnisse bei mobilen Geräten besonders durch Verlust und Diebstahl der entsprechenden Geräte. Oft genannte Konsequenzen solcher Störungen im Betriebsablauf sind Zeit- und Produktivitätsverluste (67 Prozent), technische Einschränkungen (17,2 Prozent), Aufwendungen für die Reparatur (7 Prozent) und Imageschäden für das betroffene Unternehmen (6 Prozent). Von den mehr als 1.700 befragten Unternehmen führen 13 Prozent der Unternehmen nach einer Störung der Informationssicherheit verbesserte Sicherheitsmaßnahmen wie Softwareupdates oder aber die Beauftragung externer Experten ein, während 55 Prozent der Unternehmen nach Vorfällen keine Maßnahmen einleiten oder zusätzliche Investitionen tätigen (INTECO 2012a).

Das INTECO (2012a) verweist mit Blick auf den aktuellen Stand der Informationssicherheit in spanischen KMU auf die Nutzung von Antivirensoftware in 96,1 Prozent und die Verwendung von Firewalls in 75,4 Prozent der befragten Unternehmen. 56 Prozent der KMU in Spanien greifen entweder auf internes (21 Prozent) oder externes (35,3 Prozent) Personal zurück, das sich mit Informationssicherheit beschäftigt (INTECO 2012b). Die Hälfte der Unternehmen nimmt eine Beschränkung der Installationsrechte vor und 95 Prozent führen regelmäßig Datenbackups durch. Technisch deutlich aufwendigere Sicherheitsmaßnahmen wie Datenverschlüsselung werden hingegen nur von einem Drittel der untersuchten Unternehmen eingesetzt.

Obwohl laut der Erhebung durch das INTECO (2012a) das Thema Informationssicherheit von mehr als 70 Prozent des Managements der spanischen KMU als „sehr wichtig“ oder „wichtig“ bewertet wird, führen nur 27 Prozent der spanischen KMU Schulungen für Mitarbeiter im Umgang mit Sicherheitsrisiken durch und auch die Implementierung von Betriebskontinuitätsplänen ist bisher mit knapp 32 Prozent der befragten Unternehmen allenfalls geringfügig verbreitet.

Mit Blick auf die große Bedeutung, die dem Thema Informationssicherheit vom Management in KMU zugeschrieben wird, stellt sich die Frage, warum Maßnahmen zur Prävention von Schäden und Störungen der Informationssicherheit nicht implementiert werden. Eine weitere Erhebung durch das INTECO (2008) führte neben nicht ausreichenden personellen und finanziellen Ressourcen in KMU, geringe technische Kenntnisse bei Angestellten und Firmenleitung sowie ein mangelndes Bewusstsein für die Bedeutung der betrieblichen Informationssicherheit an. Mangelndes Bewusstsein entsteht unter anderem auch durch das im Vergleich zu großen Unternehmen geringere Angebot zum Aufbau von Kenntnissen zum Thema Informationssicherheit und resultiert in einem möglicherweise fahrlässigen Umgang mit den vorhandenen IT-Systemen durch die Mitarbeiter. Zudem führten spanische KMU das aus ihrer Sicht mangelnde Angebot an speziell auf die Bedürfnisse der KMU zugeschnittenen Produkten und Dienstleistungen zur Verbesserung der Informationssicherheit an (INTECO 2008). Die Anschaffung neuer Sicherheitstools scheitert laut Untersuchung des INTECO (2012a) an der mangelnden Kenntnis des Produktes (zum Beispiel Anti-Intrusion Systeme) oder aber der Überzeugung, bestimmte Produkte nicht zu benötigen.

5.6.3 Initiativen zur Informationssicherheit

Spanien adressiert das Thema der Cybersicherheit ebenfalls mit einer eigenen Strategie. In der Nationalen Sicherheitsstrategie (*Estrategia Espanola de Seguridad Nacional 2013*) wird das Thema Cybersicherheit bereits als eines der Zwölf Kernhandlungsfelder identifiziert. Der Nationalen Sicherheitsstrategie nachgeordnet ist die Nationale Cybersicherheitsstrategie (*Estrategia de Ciberseguridad Nacional 2013*), Bei dieser handelt es sich um ein allgemein

gehaltenes Dokument, dass nicht explizit KMU aufführt und auch andere Unternehmen nur peripher adressiert.

Im Kontext dieser Strategie steht das zum Ministerium für Industrie, Energie und Tourismus gehörende *Instituto Nacional de Tecnologías de la Comunicación* (INTECO). INTECO bietet im Bereich Cybersicherheit Dienstleistungen an und betreibt Forschung auf diesem Gebiet. Es scheint zunächst, dass INTECO Mittelstandspolitik betreibt. Tatsächlich verfolgt es im Sinne der Cybersicherheitsstrategie (s.o.) eher geostrategische Ziele. Darüber hinaus koordiniert INTECO nationale Initiativen und Ansätze und arbeitet mit nationalen und internationalen Partnern zusammen. INTECO existiert seit 2006 und wächst seitdem stetig. In diesem Jahr soll die Hundertmitarbeitermarke erreicht werden.

Im Jahr der Gründung von INTECO wurde der Betrieb des *INTECO-CERT* aufgenommen. Das *INTECO-CERT* stellt neben seinen Benachrichtigungen über aktuelle Cyberbedrohungen und mögliche Schutzmaßnahmen Informationen zum Thema Rechtsberatung und Störungsmanagement zur Verfügung. Im Jahr 2013 wurden dem *INTECO-CERT* 54.000 Sicherheitsvorfälle gemeldet und die Website knapp 6,5 Millionen Mal aufgerufen. Durch ein durchgeführtes Experteninterview konnte in Erfahrung gebracht werden, dass keinesfalls nur spanische Unternehmen und Bürger auf die Dienste des *INTECO-CERT* zugreifen, sondern auch Unternehmen und Bürger aus dem spanisch sprachigen Ausland sowie die hispanischen Einwohner der USA.

Zusätzlich zum *INTECO-CERT* bietet INTECO seit 2013 auf seiner Website speziell für KMU ein Programm an, mit dem Informationsmaterialien und Trainingsangebote bereitgestellt werden. Dabei wird der Fokus darauf gelegt Unternehmen, die keine IT-Expertise besitzen, mit allgemein verständlichen Informationen zu versorgen und ihnen somit die Möglichkeit zu geben ohne großen Aufwand ihre IT-Sicherheit zu verbessern.

Das *Industrial Cybersecurity Center* (Centro de Ciberseguridad Industrial) CCI wurde im Juni 2013 gegründet und thematisiert industrielle Cybersicherheit in Lateinamerika und Spanien. Unternehmen können auf unterschiedlichen Stufen als Mitglieder partizipieren und entsprechenden Zugriff auf Dokumente und Veranstaltungen erhalten. Das CCI ist mit der Maxime angetreten, den Mangel an spanisch sprachigen Dokumenten zum Thema IT-Sicherheit zu beheben. Neben Trainings von unterschiedlicher Dauer und Umfang stellt das CCI seinen Mitgliedern exklusiv kostenpflichtige Dokumente und Verfahrensanweisungen zur Verbesserung der IT-Sicherheit im Unternehmen bereit, wobei diese sich an Standards wie ISO27002 orientieren Die auch für Externe frei erhältliche Cybersicherheits-Roadmap wurde bereits 30.000 Mal heruntergeladen. Der vom CCI organisierten Kongress *Voice of the Industry* hat zum Ziel, den wachstumsstarken Markt für IT-Sicherheit zu vergrößern und sowohl national als auch international neue Geschäftsfelder zu erschließen.

Das 2007 gegründete *ISMS Forum* (Asociación Española para el Fomento de la Seguridad de la Información) verbindet Stakeholder aus Unternehmen, öffentlichen Organisationen und Einrichtungen und Fachleuten um die Informationssicherheit in Spanien zu erhöhen. Im Januar 2013 organisierte das *ISMS Forum* unter der Mithilfe zahlreicher Partner wie INTECO, Deloitte und anderen großen Unternehmen eine umfangreiche Cyberübung, bei der die IT-Infrastruktur eines Unternehmens einem Penetrationstest unterzogen werden. Um sich dabei juristisch abzusichern werden im Vorfeld Verträge abgeschlossen um die Angriffe durch die Hacker zu autorisieren. Bis dato wurden diese Angriffe allerdings nur auf Unternehmen des ersten spanischen Aktienindexes (IBEX 35) durchgeführt. Durch ein Interview mit dem Präsidenten des *ISMS Forum* konnte jedoch eruiert werden, dass es Pläne gibt, diese Übungen auf KMU auszuweiten.

5.6.4 Wesentliche Erkenntnisse

Spanien verfolgt ähnlich wie Schweden sowohl geostrategische Ziele als auch die Förderung des Mittelstands. Im Mittelpunkt stehen allerdings der Schutz der kritischen Infrastruktur und die Wahrung der geostrategischen Interessen. Dabei wird dennoch versucht, mittelständische Unternehmen einzubeziehen.

5.7 USA

5.7.1 Kurzüberblick

Struktur der kleinen und mittelständischen Unternehmen (in den USA bis zu 500 Angestellte)

			[27]
Mittlere Unternehmen (100-499 Angestellte)	88.586	17.173.728	2.652 Mrd. €
Kleinunternehmen (10-99 Angestellte)	1.177.233	29.579.142	3.808 Mrd. €
Kleinstunternehmen (0-9 Angestellte)	26.473.646	13.114.054	2.622 Mrd. €
Summe	**27.739.365**	**59.866.924**	**9.082 Mrd. €**
Anteil an Gesamtwirtschaft	99,9 Prozent	49,9 Prozent	40,3 Prozent

Quelle: https://www.census.gov/econ/smallbus.html (Stand 2007)

Bedeutung und Stand der Informationssicherheit	• Mehr als 70 Prozent der amerikanischen Unternehmen gaben 2010 an, im vergangenen Jahr Opfer von Cyberangriffen geworden zu sein.
Wesentliche Akteure und Initiativen	• Die *Federal Communications Commission* (FCC) stellt den *Small Biz Cyber Planner 2.0 zur Verfügung* • Die *U.S. Small Business Administration* (SBA) ist zuständig für die Initiative *Cybersecurity for Small Businesses* • SBA, FBI und NIST unterhalten gemeinsam den *Small Business Corner*

5.7.2 Bedeutung und Stand der Informationssicherheit

Laut Internet Security Alliance (2013) hat die in den vergangenen Jahren erfolgte Aufrüstung großer amerikanischer Unternehmen bei der Implementierung von umfassenden Sicherheitsmaßnahmen zum Schutz ihrer betrieblichen Informationssicherheit dazu geführt, dass sich der Fokus externer Attacken zunehmend von großen Unternehmen hin zu amerikanischen KMU verschoben hat.

Angriffe auf die Informationssicherheit von amerikanischen KMU besitzen ein zunehmend größeres Schadenspotential. Die „fortgeschrittene andauernde Bedrohung“ (Advanced Persistent Threat), ist somit für eine Vielzahl von amerikanischen KMU in den letzten Jahren Realität geworden. Die Wahrnehmung, einer gesteigerten Gefährdung von Unternehmensprozessen ausgesetzt zu sein, wird auch von den Vertretern der amerikanischen KMU geteilt, die Datenverluste und Cyber-Attacken als die mit Abstand größten Risiken für den regulären Betrieb ihrer Geschäftstätigkeit betrachten, gefolgt von Diebstahl und Naturkatastrophen. Einen Indikator für die tatsächliche Gefährdung von KMU stellen die Ergebnisse in einer von Symantec (2010) veröffentlichten Studie dar, in der mehr als 70 Prozent der befragten Unternehmen bestätigten, während des Vorjahres Opfer von Cyberkriminalität

[27] Der U.S. Census gibt anstelle des Umsatzes die *Sales or Receipts* an.

gewesen zu sein, wobei laut Erhebung etwa ein Drittel der erfolgten Angriffe erhebliche Konsequenzen für die Produktivität, Erträge und das Kundenvertrauen nach sich zog.

Während also eine große Mehrheit der Verantwortlichen in amerikanischen KMU sich der potentiellen Gefährdung der betrieblichen Informationssicherheit durch externe und interne Angriffe durchaus bewusst ist und im Durchschnitt etwa 51.000 Dollar pro Jahr für den Schutz der Informationssicherheit aufwendet (Symantec 2010), mangelt es dennoch in einer Vielzahl an KMU an konkreten, die Informationssicherheit verbessernden Maßnahmen. Nach einer Erhebung durch die National Cyber Security Alliance und Symantec (2012) besitzen 69 Prozent der Unternehmen keine formellen oder informellen Vorgaben für Mitarbeiter zum sicheren Umgang mit dem Internet und nur 14 Prozent der Unternehmen geben an, formell festgelegte Vorgaben zum Thema Cybersicherheit implementiert zu haben. Auch die Einführung von Betriebskontinuitätsplänen, die die zu treffenden Maßnahmen in Folge von Datenverlusten vorgeben, ist in weniger als einem Drittel der Unternehmen erfolgt. In der Literatur wird als eine der zentralen Ursachen für mangelnde Maßnahmen zum Schutz der Informationssicherheit die starke Inhaberzentrierung bei KMU genannt (National Cyber Security Alliance und Symantec 2012). So geben 66 Prozent der befragten Besitzer bzw. Geschäftsführer an, dass ausschließlich sie für Online- und Cybersicherheit verantwortlich sind, während ein geringer Teil internen IT-Sicherheitsexperten vertraut (9 Prozent), beziehungsweise externe IT-Sicherheitsexperten heranzieht (11 Prozent). Zugleich offenbart sich eine Diskrepanz zwischen der eingangs erwähnten Beeinträchtigung von Produktivität und Erträgen bei einem Drittel der erfolgten Angriffe und der zeitgleichen Einschätzung von 77 Prozent der befragten Unternehmen, mit den vorhandenen Sicherheitsvorkehrungen das Unternehmen ausreichend gegen externe und interne Angriffe und Störungen geschützt zu haben.

5.7.3 Initiativen zur Informationssicherheit

Grundlage der amerikanischen Bemühungen für eine Verbesserung von Informationssicherheit ist die *Comprehensive National Cybersecurity Initiative*. Diese wurde ursprünglich unter Präsident George W. Bush im Januar 2008 vorgestellt und von seinem Nachfolger Barack Obama weiterverfolgt und ausgebaut. Obama bezeichnete Cyberbedrohungen als eine der schwerwiegendsten Herausforderungen für die US-Wirtschaft sowie die nationale Sicherheit. Bei der im Zuge des *National Cyber Security Awareness Month* im Oktober 2010 vorgestellten *Stop Think Connect* Kampagne handelt es sich um eine Bewusstseinsförderungskampagne die von Unternehmen, Non-Profit Organisationen und Regierungsorganisationen unter der Schirmherrschaft der *National Cyber Security Alliance* (NCSA) und der *Anti-Phishing Working Group* (APWG) entwickelt wurde.

Initiativen zur Verbesserung der Informationssicherheit in KMU werden in den USA von verschiedenen nationalen, als auch regionalen Akteuren getragen. Einen der Impulsgeber für konkrete Initiativen im Kontext der Informationssicherheit stellt das D*epartment of Homeland Security* (DHS) dar. Das DHS wurde 2002 unter dem Eindruck der Terroranschläge des 11. September 2001 geschaffen. Zu den 15 Themen, die unter dem Dach des DHS behandelt werden, gehört auch das Thema Cybersicherheit. Das dem DHS unterstellte *United States Computer Emergency Readiness Team* bietet KMU an, sie regelmäßig über Sicherheitswarnungen und Verhaltenstipps via E-Mail oder SMS zu informieren.

Die *Federal Communications Commission* (FCC) ist ebenfalls im Bereich IT-Sicherheit involviert. Als unabhängige US Regierungsbehörde, die vom Kongress überwacht wird, ist sie federführend für Kommunikationsgesetzgebung, Regulierung sowie technologische Innovationen. Die Aufsichtsbehörde der FCC ist das *Department of Comm*erce. Mit dem

Small Biz Cyber Planner 2.0 gibt die FCC Unternehmen die Möglichkeit auf Basis von Unternehmensspezifika einen individualisierter Plan zur Verbesserung der IT-Sicherheit im jeweiligen Unternehmen zu erzeugen. Die Möglichkeiten zur Individualisierung sind jedoch nur eingeschränkt, so erfolgt die Auswahl der Kapitel mittels 12 Kriterien. Zusätzliche inhaltliche Beiträge bei der Entwicklung kam außerdem vom Department of Homeland Security, der NCSA, dem *Department of Commerce* sowie großen Unternehmen wie VISA, Symantec und Microsoft. Der *Small Biz Cyber Planner 2.0* existiert seit Oktober 2012.

Die *US Small Business Administration* (SBA), eine Regierungsbehörde die Unternehmer und kleine Unternehmen durch Kredite, Beratung etc. unterstützen soll, hat die Initiative *Cybersecurity for Small Businesses* ins Leben gerufen. Die am 31.10.2013 gestartete Initiative besteht aus einem Webcast, in dem KMU in 30 Minuten grundlegende Informationen zum Thema Cybersicherheit erhalten. Als Teilnahmebestätigung kann im Anschluss ein Zertifikat heruntergeladen werden, durch das das Absolvieren des Webcasts nachgewiesen werden kann. Die SBA hat als landesweit agierende Behörde Dependancen in jedem Bundesstaat und ist somit in der Lage, landesweite Kampagnen durchzuführen bzw. administrativ zu unterstützen.

Dieses Netzwerk kommt der Initiative *Small Business Corner* zu Gute, die durch ein sogenanntes „Interagency Agreement“ zwischen der SBA, dem *National Institute of Standards and Technologies* (NIST) und dem *Federal Bureau of Investigation* (FBI) durchgeführt wird. Während das NIST, die dem *Department of Commerce* zugehörige Behörde für Standards und Technologien die Workshops durchführt, kümmern sich SBA und FBI um die administrativen Tätigkeiten. Im Zuge der Initiative werden landesweit Workshops durchgeführt, die KMU in 4 Stunden einen Überblick über IT-Sicherheit, mögliche Cyberbedrohungen und Tools und Techniken zur Gefahrenabwehr vermitteln. Die Planungen für die Initiative begannen 2000 und nach einigen Pilotworkshops im Jahr 2001 wurde 2002 der reguläre Betrieb aufgenommen. Versucht wird die Workshops gleichmäßig über das Land zu verteilen. Es besteht aber ebenfalls die Möglichkeit, dass ein Kongressabgeordneter anfragt, ob in seinem Wahlkreis ein Workshop durchgeführt werden könnte.

Darüber hinaus existieren neben diesen bundesweiten Initiativen auf regionalem bzw. lokalem Level weitere Initiativen. Ein Bespiel hierfür ist *Securing our eCity* aus San Diego. Die Initiative wird von der *ESET Stiftung* betrieben, die von der Softwaresicherheitsfirma *ESET LLC* in San Diego gegründet wurde. Darüber hinaus existieren sogenannte Sponsoren und Partner („Donors“ und „Partners“) die zum Erfolg der Initiative beitragen (u.a. verschiedene Unternehmen und städtische Einrichtungen, z.B. das *San Diego Police Department*. Die Initiative richtet sich sowohl an öffentliche Einrichtungen als auch an KMU und sogar Privatpersonen. Im Vorfeld werden gemeinsam mit den Rezipienten der Workshops die spezifischen Anforderungen abgestimmt und der Workshop entsprechend aufgebaut. Im Nachgang findet dann mit den Teilnehmern eine Evaluation statt, wo erfasst wird, inwiefern der abgehaltene Workshop ihr Verhalten geändert hat.

Auch auf einer dem Bundesstaat untergeordneten Verwaltungseinheit der USA, dem County, gibt es Initiativen zur Förderung der IT-Sicherheit. Im Howard County in Maryland hat das *Howard Tech Council* die *HoCo CISO* Initiative ins Leben gerufen. Die im Howard County angesiedelten IT-Unternehmen stellen den KMU pro-bono einen *Chief Information Security Officer* (CISO) in einer virtuellen Umgebung zur Verfügung. KMU erhalten so Beratung durch IT-Sicherheitsexperten, zu denen sie andernfalls keinen Zugriff hätten.

5.7.4 Wesentliche Erkenntnisse

In den USA stellte es sich aufgrund der durch die Geschehnisse um die NSA-Affäre belasteten Beziehungen zwischen Deutschland und den USA teilweise als kompliziert heraus, mit Vertretern von Regierungsinstitutionen über nationale Initiativen zur Förderung der Informationssicherheit zu sprechen.

Eine mit Deutschland vergleichbare auf KMU konzentrierte Unterstützung auf Regierungsebene ist in den USA so nicht vorhanden. Nachgeordnete nationale Behörden verteilen vor allem allgemeine Informationen und Materialien zur Informationssicherheit. Lediglich die Workshops des *Small Business Corner* sprechen KMU direkt vor Ort an. Den direkten Kontakt zu den Unternehmen suchen ansonsten eher lokale Initiativen.

6 Handlungsoptionen

Die Vergleichsanalyse und die Länderberichte zeigen unterschiedliche Rahmenbedingungen und verschiedene Ansätzen, weisen aber ebenso auf eine Reihe von Gemeinsamkeiten hin, woraus sich mögliche Anknüpfungspunkte für zukünftige Initiativen des BMWi ableiten lassen. Zu diesem Zweck werden die detaillierten Informationen aus der Erfassung in die fünf Phasen überführt, die ein Unternehmen von der ersten Vertiefung des Themas bis hin zur Bewältigung von Angriffen durchläuft:

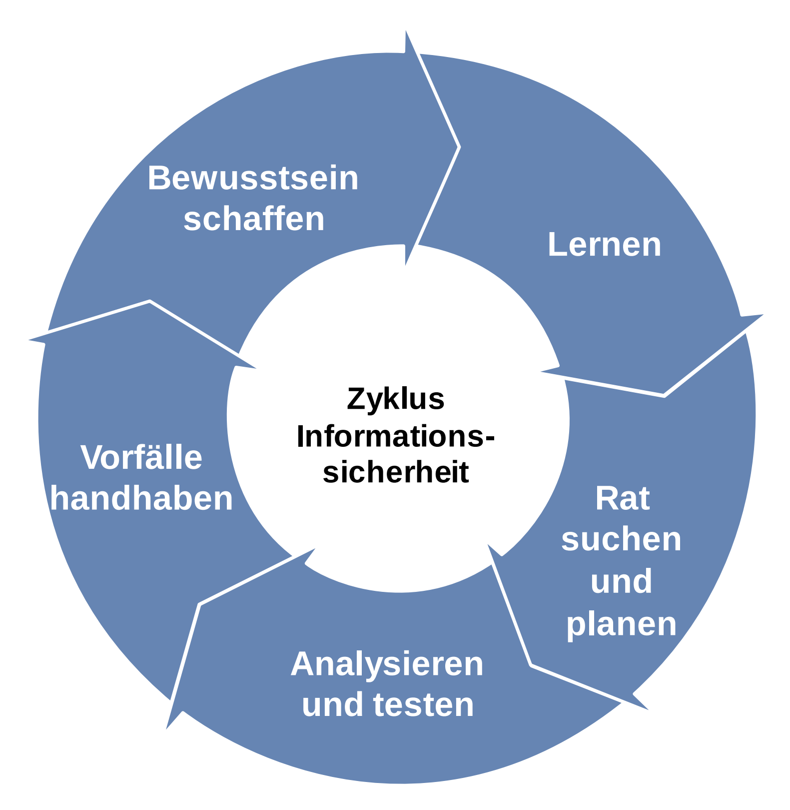


Abbildung 40: Zyklus zur Schaffung von Informationssicherheit

Unternehmen absolvieren diesen Zyklus nicht einmalig, sondern mit jeder neuen Bedrohung, durch Kollegen, Branchennachrichten, Marktinformation oder konkrete Ereignisse getrieben. Eine Bedrohung kann aus dem Einsatz neuer Technologien (z.B. Cloud Computing) oder einer geänderten Gefahrensituation (z.B. neue Methoden der Kommunikationsüberwachung) resultieren. Insofern sind zur Erarbeitung von Handlungsoptionen auch die Initiativen zu den Phasen am Anfang des Zyklus (Bewusstsein schaffen und Lernen) von Interesse, die, wie zu erwarten, den größten Anteil (42 der 56 Initiativen) an den untersuchten Initiativen ausmachen:

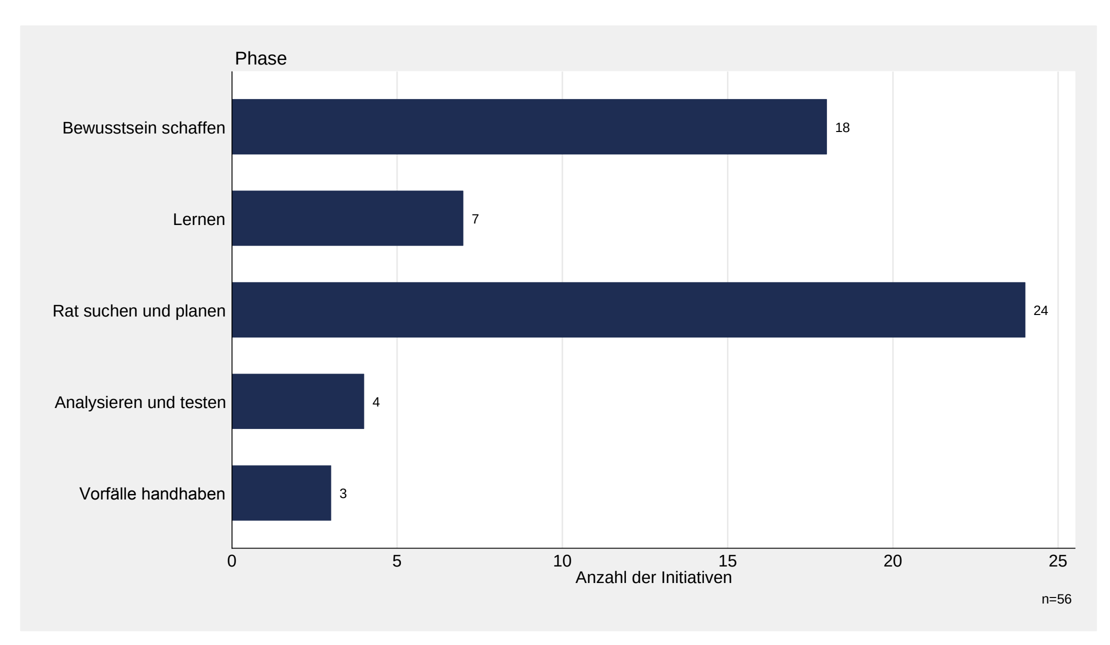


Abbildung 41: Die Initiativen nach Phasen im Überblick

Die Verteilung der Initiativen nach Phasen im Zyklus illustriert nochmals das Ergebnis der Vergleichsanalyse, wonach der Schwerpunkt derzeit noch bei den Empfehlungen zur Steigerung der IT-Sicherheit in KMU liegt. Wie Abbildung 42 zeigt, stehen alle untersuchten Länder vor der Herausforderung, nach der Schaffung des erforderlichen Bewusstseins und grundsätzlichen Wissens über mögliche Maßnahmen zur Verbesserung der Informationssicherheit in ihren Unternehmen KMU bei der Implementierung dieser Maßnahmen konkret zu unterstützen.

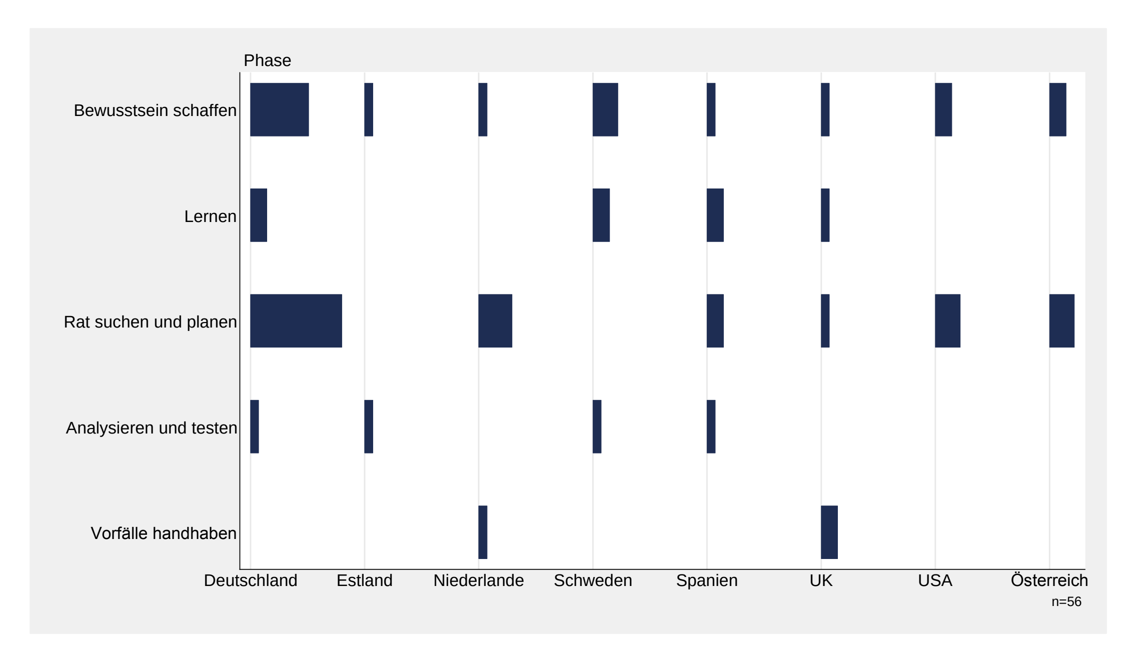
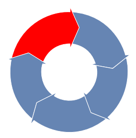


Abbildung 42: Die Initiativen nach Phasen und Ländern

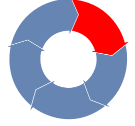
Im Folgenden werden entlang der fünf Phasen Handlungsoptionen anhand der jeweils zugeordneten Initiativen erarbeitet.



6.1 Phase 1: Bewusstsein schaffen

Zu den Initiativen, die das Bewusstsein für Sicherheit in der IT bei KMU stärken, gehören Informationsangebote, Kampagnen und Schulungen, die verzerrte Wahrnehmungen der Unternehmenslenker korrigieren. Wie erfolgreich die einzelnen Initiativen tatsächlich dabei sind, ließe sich allenfalls mittels aufwändiger Erhebungen durch die Initiatoren ermitteln, die jedoch nicht vorliegen. Dennoch zeigen die Gespräche mit den Experten, dass eine staatliche Initiative umso eher die Unternehmen erreicht, je gezielter die Ansprache der jeweiligen Zielgruppe in ihrem entsprechenden Reifegrad erfolgt. Einen Hinweis für diese These liefert insbesondere die schwedische *Info-Tour*, die mangels belegbaren Erfolgs eingestellt wurde. Diese Initiative fokussierte sich weder auf Unternehmen noch auf bestimmte Themen und war ohne definiertes Ziel, wie im Interview festgestellt wurde.

Andere Initiativen, die gezielt einzelne KMU an das Thema Informationssicherheit heranführen, scheinen zwar eine bessere Resonanz zu haben, allerdings erreichen diese aufgrund der klar begrenzten Zielgruppe wenige Unternehmen. Mehr Unternehmen erreichen Initiativen wie die Internetportale zur Informationssicherheit, deren Angebote nicht sicherstellen können, dass die Besucher der Websites ein Bewusstsein entwickeln. Einen Ausweg aus diesem (Reichweite und Reichtiefe) Dilemma ist aus die Einbindung von Multiplikatoren bieten, die die vorhandenen Informationen ihren Klienten, Kunden oder Mitgliedern nahebringen. Entscheidend für den Erfolg ist dabei die Nähe zum Unternehmen, weshalb sich insbesondere in Deutschland die Berater in den Kammern in Zusammenarbeit mit den regionalen IT-Dienstleistern anbieten. Ebenso geeignet können besonders vertrauenswürdige Personen sein, sofern diese in einer kontinuierlichen Geschäftsbeziehung zum Unternehmen stehen.

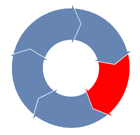


6.2 Phase 2: Lernen

Angesichts der hohen Anzahl an Lernangeboten verwundert die vergleichsweise geringe Zahl von Initiativen in dieser Phase auf den ersten Blick. Allerdings steht bei einigen Schulungen und Workshops weniger das Erlernen konkreter IT-Inhalte, sondern mehr die Bildung des Bewusstseins im Vordergrund. Folglich bleibt den Interessierten zur Bildung von IT-Sicherheitskompetenzen auf der technischen Ebene nur die Wahl eigener Initiativen.

Die Angebote, die konkrete und praktizierbare Lerninhalte vermitteln, stehen der Herausforderung gegenüber, möglichst viele KMU mit möglichst wenig Aufwand zu erreichen. Ein dazu in Großbritannien und Deutschland gewählter Ansatz besteht in der Nutzung von E-Learning-Plattformen, also der Vermittlung von Wissen auf Basis elektronischer Informations- und Lernsysteme. Vorteile dieses Ansatz liegen zum einen darin, dass die Teilnehmeranzahl nicht durch Räumlichkeiten limitiert ist, eine relative freie Terminwahl, Abrufen beliebiger Inhalte zur Wunschzeit des Lernenden und zum anderen senkt der virtuelle Seminarraum die Kosten für Teilnahme zum Beispiel zur Anfahrt an den Schulungsort. Dennoch erfordern Internet basierte Seminare (Webinare) ein Minimum an finanziellem Aufwand, der aber in Großbritannien nach der staatlichen Anschubfinanzierung durch Gebühren gedeckt werden kann. Dass grundsätzlich auch kleine Unternehmen bereit sind,

einen kleinen Obolus zu leisten, zeigen die bereits seit 1996 laufenden Kurse an der schwedischen KTH.



6.3 Phase 3: Rat suchen und planen

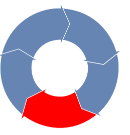
Initiativen, die sich der dritten Phase zuordnen lassen, versuchen in erster Linie die fehlenden Ressourcen und lückenhaftes Wissen der Inhaber zu kompensieren. Indem sie KMU vor allem Dienstleistungen anbieten, wird zudem das Problem der mit der Verbesserung der IT-Sicherheit einhergehenden Kosten aufgegriffen. Diese Leistungen gliedern sich – von wenigen Ausnahmen in Deutschland abgesehen – in erstens interaktive Informationsangebote, zweitens die Leistungen von CERTs sowie drittens individuelle Beratungen vor Ort.

Interaktive Informationsangebote finden sich in Deutschland mit dem *DsiN-Sicherheitscheck*, und *ISA+,* in den USA mit dem *Small Biz Cyber Planner*, in den Niederlanden mit dem *Cyberscan* und in Österreich auf dem Portal *it.safe.at*. Dabei fokussiert der Ansatz in den USA und in Österreich auf eine allgemein anerkannte Richtlinie, deren Anwendung durch das jeweilige interaktive Tool erleichtert werden soll. Diese Fokussierung – sowie in Österreich möglicherweise auch die Nähe der Wirtschaftskammer zu den Unternehmen – scheint zumindest eine positive Wirkung im Hinblick auf die Ansprache der Unternehmen zu haben. Die Initiative *ISA+*, die derzeit noch im Aufbau ist, verfolgt einen ähnlichen Ansatz, bietet aber darüber hinaus ein Zertifikat.

Die Leistungen von CERTs stehen KMU direkt oder indirekt in Deutschland, Spanien, den Niederlanden und Österreich zur Verfügung. In den USA und in Großbritannien hingegen waren ähnliche Angebote an KMU nicht erkennbar und in Estland sogar ausdrücklich ausgeschlossen. Die Länder, in denen KMU die Angebote der CERTs prinzipiell offen stehen, bemühen sich, KMU gezielt anzusprechen. Dennoch zeigen sich in der Umsetzung die Herausforderungen, kleinen Unternehmen, die über keine ausgeprägte IT-Expertise verfügen, die Vielzahl technischer Informationen bedarfs- und praxisgerecht anzubieten. Das hier vorhandene Potenzial wird von den Entscheidungsträgern durchaus erkannt, wie die Diskussion in Österreich über die Möglichkeiten, die Informationen des CERT's im Hinblick auf die spezifischen Belange von KMU aufzubereiten, zeigt. Konkrete Planungen dazu liegen jedoch noch nicht vor.

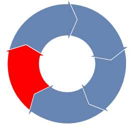
Individuelle Beratungen vor Ort werden entweder direkt durch Mitarbeiter der jeweiligen Initiative oder, wie derzeit in Großbritannien und zuvor in Österreich, mit Hilfe von staatlichen Zuschüssen durch IT-Dienstleister erbracht. In beiden Fällen bedarf es eines Budgets, das die Zahl der möglichen Beratungen beschränkt. Daher ist der Ansatz der britischen *Innovation Vouchers for Cyber Security*, die Vergabe der Mittel an KMU mit Bedingungen zu verknüpfen, für eine mögliche Adaption von besonderem Interesse. Insbesondere die Anforderung, die Idee und Umsetzung des Vorhabens zu erläutern, könnte einen Beitrag zur optimalen Allokation der begrenzten Ressourcen leisten. Vor einer Umsetzung wäre zu überlegen, weitere Anforderungen an die Dienstleistung, z.B. in Form eines Pflichtenheftes, oder einer „Zertifizierung" zu formulieren. Langfristig erhofft sich Großbritannien durch die Förderung den Aufbau eines Netzwerks von IT-Dienstleistern und KMU. Dieses Ziel hat auch die Initiative in Nordrhein-Westfalen, wobei Dienstleister und Unternehmenskunden jedoch nicht mit Hilfe von Zuschüssen, sondern durch die Finanzierung einer Plattform

zusammenfinden sollen, indem die Dienstleister ihre Beratung in Form eines Angebots zur Verfügung stellen.



6.4 Phase 4: Analysieren und testen

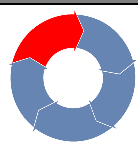
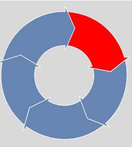
In Gesprächen mit verschiedenen Trägern kam deren Wunsch zum Ausdruck, nach erfolgreicher Ansprache der Zielgruppe derselben konkrete Lösungen an die Hand geben zu können. Viele Gesprächspartner sind der Ansicht, dass – nicht zuletzt infolge der NSA-Affäre – auch mittelständische Unternehmen mittlerweile ein deutlich höheres Bewusstsein für das Thema der Informationssicherheit entwickelt haben. Infolgedessen sei ein Bedarf nach geeigneten Lösungen geweckt worden. Solche Lösungen werden jedoch bislang nur von wenigen Initiativen angeboten. Von diesen Initiativen wiederum ist lediglich die *Initiative-S* tatsächlich aus Sicht Mittelstand definiert worden. Die Initiativen in Spanien und Schweden erfassen eine (kleine) Zahl von Unternehmen, zu denen zwar grundsätzlich KMU gehören können, der Fokus jedoch liegt auf der kritischen Infrastruktur. Inwieweit der doch verfolgte Ansatz sich auf eine breitere Gruppe von KMU übertragen lässt, ist schwer einzuschätzen. Die spanischen Überlegungen dazu sind zumindest bislang noch nicht konkretisiert worden. Insofern ist der deutsche Ansatz, sich auf einen Teil der Unternehmenssysteme zu konzentrieren, erfolgversprechender. Da die *Initiative-S* mit ihrem Siegel dem Unternehmen, ähnlich wie mit einer Zertifizierung, einen öffentlichkeitswirksamen Anreiz geben will, könnte hier die Möglichkeit für eine Integration in einen zertifizierten Standard überlegt werden, wozu sich beispielsweise die Initiative *ISA+* anbietet.

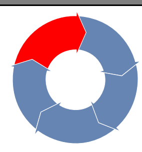


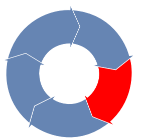
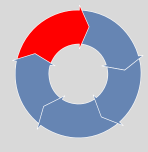
6.5 Phase 5: Vorfälle handhaben

Die Initiativen in Großbritannien, die KMU nach Eintreten eines Vorfalls Unterstützung, lassen sich am ehesten vergleichen mit der Beratung durch die Polizeidienststelle nach einem Wohnungseinbruch. Dementsprechend sind in Großbritannien auch die regionalen Polizeibehörden Partner der jeweiligen Initiative. Einen stärker standardisierten und in der Außenwirkung innovativeren Ansatz haben die Niederlande gewählt, indem sie auf der Website nach Themen unterteilte „Notfallschalter" anbieten. Prinzipiell besteht auch in Deutschland die Möglichkeit, sich nach einer Attacke an die Sicherheitsbehörden zu wenden. Von dieser Möglichkeit scheinen jedoch KMU nur selten Notiz zu nehmen. Wichtiger ist wohl zunächst einmal die Schadensbegrenzung mit Hilfe des eigenen IT-Dienstleisters. Ein denkbarer Ansatz könnte daher sein, eine engere Verknüpfung der Sicherheitsbehörden mit den IT-Experten der KMU herzustellen.

Anhang A: Übersicht der untersuchten Initiativen

Land	Beschreibung
 **DE**	**[m]IT Sicherheit – Bewusstseinsbildung für IT-Sicherheit in KMU**  **Laufzeit** 15. Juni 2012 bis 31. Dezember 2013 **Ansatz:** Die Initiative hatte zum Ziel über verschiedene Wege KMU für das Thema IT-Sicherheit zu sensibilisieren. Dazu gehörten eine Roadshow mit Vorträgen, Diskussionen und Live-Hacking sowie eine Broschüre mit Fallbeispielen und weitere von durch den Verband organisierten Experten erstellte Informationsmaterialien, Des Weiteren wurde Unternehmen über die Website der Initiative die Teilnahme an einem Sicherheitscheck angeboten. Außerdem versuchte die Initiative Verbände und Institute der Kreditwirtschaft als Multiplikatoren zu gewinnen. **Kontakt:** Alexandra Horn Bundesverband mittelständische Wirtschaft, Unternehmerverband Deutschlands e.V. (BVWM) Leipziger Platz 15, 10117 Berlin Tel: 0049 30 533206-57 / E-Mail: alexandra.horn@bvmw.de **Webseite:** http://www.mit-sicherheit.bvmw.de
 **DE**	**Online-Seminare für IT-Sicherheit in KMU**  **Laufzeit:** 15. Oktober 2012 bis 31. Dezember 2013 **Ansatz:** Die *Bitkom Akademie* organisierte im Rahmen der Initiative IT-*Sicherheit in der Wirtschaft* vom BMWi geförderte Webinare. Dazu wurden Referenten aus Unternehmen gewonnen, die durch die *Bitkom Akade-mie* zum Online-Referenten ausgebildet wurden. Die circa einstündigen Seminare sind gezielt auf einzelne Gruppen von Mitarbeitern bei KMU (Inhaber bzw. Manager, IT-Verantwortliche und Mitarbeiter ohne besondere IT-Kenntnisse) ausgerichtet worden. Die Online-Seminare werden derzeit auch nach Auslaufen der Förderung weiterhin kostenlos angeboten. **Kontakt:** Johanna Steinfeld Bitkom Servicegesellschaft mbH Albrechtstraße 10, 10117 Berlin Tel: 0049 30 27576-156 / E-Mail: j.steinfeld@bitkom-service.de **Webseite:** http://www.bitkom-akademie.de/seminare/it-sicherheit

Land	Beschreibung
 **DE**	 **Posterkampagne zur Sensibilisierung von Mitarbeitern in Unternehmen** **Laufzeit:** Die Kampagne läuft seit 2013. **Ansatz:** Die Initiative *IT-Sicherheit in der Wirtschaft* bietet KMU Poster zum Anbringen in den Unternehmensräumen sowie ergänzende Materialien an, die kostenlos direkt beim BMWi bezogen werden können. Die Poster sollen plakativ auf verschiedene Gefahrenquellen und einfache Verhaltensregeln hinweisen. **Kontakt:** Marco Schuldt Bundesministerium für Wirtschaft und Energie Villemombler Str. 76, 53123 Bonn Tel: 0049 30 18615-3228 / E-Mail: marco.schuldt@bmwi.bund.de **Webseite:** http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Angebote/sensibilisierungskampagne.html
 **DE**	**Bürger-CERT** **Laufzeit:** Das *Bürger-CERT* wurde im Jahr 2006 als ein Gemeinschaftsprojekt des BSI und *Mcert Deutsche Gesellschaft für IT-Sicherheit* gestartet. Seit Juni 2007 werden die Dienstleistungen des *Bürger-CERT* allein durch das BSI bereitgestellt. **Ansatz:** Das *Bürger-CERT* informiert und warnt über ein Abonnement Bürger und kleine Unternehmen vor Viren, Würmern und anderen Sicherheitslücken. Die Experten des BSI analysieren und bewerten rund um die Uhr die Sicherheitslage im Internet und verschicken bei konkretem Handlungsbedarf aufgrund von Sicherheitslücken Warnmeldungen und Sicherheitshinweise per E-Mail. Des Weiteren werden mit Extraausgaben und einem Newsletter weitergehende Informationen zur IT-Sicherheit den Abonnenten zur Verfügung gestellt. **Kontakt:** Matthias Gärtner Bundesamt für Sicherheit in der Informationstechnik Godesberger Allee 185 - 189, 53175 Bonn Tel: 0049 800 2741000 / E-Mail: oeffentlichkeitsarbeit@bsi.bund.de **Webseite:** https://www.buerger-cert.de

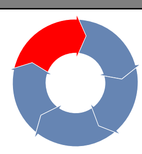
Land	Beschreibung
 **DE**	 **Deutschland sicher im Netz – Sicherheitscheck** **Laufzeit:** Der *Sicherheitscheck* wurde Oktober 2010 auf der *IT-SA* vorgestellt. **Ansatz:** Der Sicherheitscheck wird durch Mitglieder des *Deutschland sicher im Netz e.V.* betreut und im Rahmen der Initiative *IT-Sicherheit in der Wirtschaft* beworben. Bei dem Angebot handelt es sich um einen Online-Fragebogen zu verschiedenen sicherheitsrelevanten Themen im Unternehmen. Auf Grundlage der gegebenen Antworten erhält das Unternehmen eine grobe Einschätzung des Sicherheitsniveaus (Ampel) und Hinweise zur Optimierung der eigenen Informationssicherheit. **Kontakt:** Dr. Michael Littger Deutschland sicher im Netz e.V. (DsiN) Albrechtstraße 10 a, 10117 Berlin Tel: 0049 30 27576-310 / E-Mail: m.littger@sicher-im-netz.de **Webseite:** https://www.sicher-im-netz.de/machen-sie-den-dsin-sicherheitscheck
 **DE**	 **Freie Berufe als Brückenbauer** **Laufzeit:** 1. Oktober 2011 bis 31. Dezember 2013 **Ansatz:** Das durch das BMWi im Rahmen der Initiative *IT-Sicherheit in der Wirtschaft* geförderte Projekt richtete sich an Rechtsanwälte, Wirtschaftsprüfer, Steuer- und Unternehmensberater, die als Multiplikatoren die Rolle des vertrauenswürdigen Inkubators übernehmen und ihre Klienten an das Thema Informationssicherheit heranführen sollen. In drei- bis vierstündigen Workshops wurde Angehörigen dieser Berufsgruppen ein Überblick zur IT-Sicherheit, (IT-Gefahren, Nutzen als Multiplikator, Gewinn durch Investitionen in die Sicherheit), die Umsetzung eines IT-Sicherheitskonzepts, Praxisbeispiele und Lösungsansätze (Organisation der Informationssicherheit, sichere Email-Kommunikation, Datenschutz und Datensicherheit, Cloud Computing, Internet und soziale Netzwerke) vermittelt. Dazu stellten die jeweiligen Berufsverbände und andere Partner Experten als Referenten zur Verfügung und leisteten einen wichtigen Beitrag zur Akquisition der Teilnehmer. **Kontakt:** Dr. Michael Littger Deutschland sicher im Netz e.V. (DsiN) Albrechtstraße 10 a, 10117 Berlin Tel: 0049 30 27576-310 / E-Mail: m.littger@sicher-im-netz.de **Webseite:** https://www.sicher-im-netz.de/unternehmen/freie-berufe-brueckenbauer

Land	Beschreibung

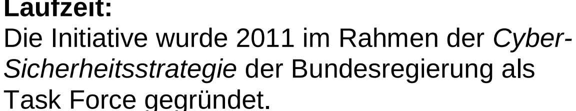


DE

Initiative "IT-Sicherheit in der Wirtschaft"



Laufzeit:



Die Initiative wurde 2011 im Rahmen der *Cyber-Sicherheitsstrategie* der Bundesregierung als Task Force gegründet.

Ansatz:

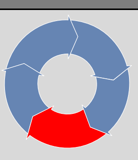
Das BMWi stellt mit dem aus Vertretern von Behörden, Verbänden, Instituten und Unternehmen bestehenden Steuerkreis den institutionellen Rahmen, der über die vom BMWi finanzierten Einzelinitiativen berät. Darüber hinaus bietet die Website der Initiative eine Vielzahl von Materialien und Informationen zu weiteren Angeboten und Initiativen sowie für KMU die Möglichkeit, an Veranstaltungen teilzunehmen oder Poster und Unterlagen zur Sensibilisierung der Mitarbeiter zu erhalten. Schließlich lässt das BMWi im Rahmen der Initiative Studien zur IT-Sicherheit in KMU anfertigen, die als Grundlage für die weitere Arbeit dienen.

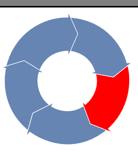
Kontakt:

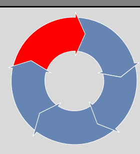
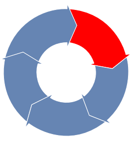
Marco Schuldt
Bundesministerium für Wirtschaft und Energie
Villemombler Str. 76, 53123 Bonn
Tel: 0049 30 18615-3228 / E-Mail: marco.schuldt@bmwi.bund.de

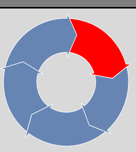
Webseite:

http://www.it-sicherheit-in-der-wirtschaft.de

Land	Beschreibung
 DE	**Initiative-S**  **Laufzeit:** 1. Juni 2012 bis 31. Dezember 2014 **Ansatz:** Unternehmen melden sich über die Website der Initiative, die vom Verband der deutschen Internetwirtschaft betreut und durch das BMWi gefördert wird, für den Check ihrer Website an. Nach der Validierung der Daten beginnen die Sicherheitsexperten des Verbands mit der Überprüfung des Webauftritts auf Schadprogramme und andere bösartige Veränderungen an der Webseite und wiederholen diese Prüfung in regelmäßigen Abständen. Hierfür kommen sowohl diverse namhafte Antiviren-Programme zum Einsatz als auch eigene Entwicklungen, um eine hohe Erkennungsrate zu gewährleisten. Entdecken die Sicherheitsexperten eine Infektion, ein Defacement oder eine Phishing-Seite, erhält das Unternehmen eine E-Mail mit ersten Informationen zur Bereinigungen der Webseiten und im Bedarfsfall der Firmenrechner. Zusätzlich enthält die E-Mail eine Ticket-Nummer und Kontaktdaten von den Experten der Initiative-S, die für Rückfragen zur Verfügung stehen sowie bei der Analyse und der Problembehebung helfen. Bei erfolgreicher Teilnahme kann das KMU mit dem "Siegel" der Initiative auf der eigenen Seite für sich werben. **Kontakt:** Markus Schaffrin eco - Verband der deutschen Internetwirtschaft e.V. Lichtstraße 43h, 50825 Köln Tel: 0049 221 700048-170 / E-Mail: markus.schaffrin@eco.de **Webseite:** https://www.initiative-s.de

Land	Beschreibung
 **DE**	**ISA+ Informations-Sicherheits-Analyse**  **Laufzeit:** Oktober 2013 bis April 2014, wobei jedoch ein Teil der Vorarbeiten bereits durch das *Projekt ISIS12* vorhanden war. **Ansatz:** Mit Förderung des BMWi erarbeitet der *Bayerische IT-Sicherheitscluster e.V.* ein IS-Managementsystem, das Kleinunternehmen eine angepasste Bedarfsanalyse ermöglicht. Mit *ISA+* erhalten auch kleine Unternehmen die Möglichkeit einer Zertifizierung. Der Fragebogen zur Analyse sowie die Empfehlungen in den Standards werden derzeit auf die Zielgruppe hin optimiert. Insbesondere durch die vorausgehende Bedarfsanalyse soll sich der individualisierte Standard an den Prozessen und den Mitarbeitern orientieren. Während der Projektlaufzeit erhalten die teilnehmenden Kleinunternehmen eine kostenlose Sicherheitsanalyse und Betreuung bei der Einführung von *ISA+* durch die Projektmitglieder. Später sollen akkreditierte IT-Dienstleister die Einführung und Zertifizierung gegen Gebühr übernehmen. **Kontakt:** Sandra Wiesbeck Bayerischer IT-Sicherheitscluster e.V. Bruderwöhrdstr. 15 b, 93055 Regensburg Tel: 0049 941 604889-18 / E-Mail: sandra.wiesbeck@it-sec-cluster.de **Webseite:** http://www.it-sicherheit-bayern.de/22/kompetenz/112260-671,1,0.html

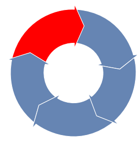
Land	Beschreibung
 **DE**	**IT-Sicherheit im Handwerk**  **Laufzeit:** 1. Oktober 2012 bis 31. Dezember 2014 **Ansatz:** Das im Rahmen der Initiative I*T-Sicherheit in der* Wirtschaft vom BMWi geförderte Projekt ist aus dem Projekt *komzet@hwk* hervorgegangen und bildet in Zusammenarbeit mit dem *Institut für Internet-Sicherheit an der Westfälischen Hochschule*, dem *Heinz-Piest-Institut für Handwerkstechnik* an der *Leibniz Universität Hannover* sowie dem *Institut für Technik der Betriebsführung im DHI e.V*. IT-Sicherheitsbotschafter aus, die als Berater in den Handwerkskammern arbeiten und in Zukunft die Handwerksunternehmen im Hinblick auf IT ansprechen, schulen und beraten sollen, u.a. auch in Form einer Veranstaltungsreihe mit mehreren Abendterminen, nach deren Besuch das Unternehmen ein Gütesiegel erwerben können soll. **Kontakt:** Dr. Giuseppe Strina Institut für Technik der Betriebsführung im DHI e.V. (itb) Kriegsstraße 103a, 76135 Karlsruhe Tel: 0049 721 93103-0 / E-Mail: strina@itb.de **Webseite:** http://handwerk.it-sicherheit.de
 **DE**	**IT-Sicherheit in der Hotellerie**  **Laufzeit:** 3. September 2012 bis 31. Dezember 2013 **Ansatz:** Der Verband *TeleTrust e.V*. und der *Hotelverband Deutschland e.V*. führten im Rahmen der Initiative *IT-Sicherheit in der Wirtschaft* mit Förderung des BMWi speziell an Beherbergungsunternehmen gerichtete Workshops zu Gefahren und Lösungen vor allem im Hinblick auf rechtliche Anforderungen zur IT-Sicherheit, Datenschutz, WLAN, Kreditkarten und Buchungssystemen durch. Die Workshops waren für die Unternehmen kostenlos und wurden durch ehrenamtliche Referenten betreut. **Kontakt:** Marieke Petersohn TeleTrusT - Bundesverband IT-Sicherheit e.V. Chausseestraße 17, 10115 Berlin Tel: 0049 30 40054-308 / E-Mail: marieke.petersohn@teletrust.de **Webseite:** https://www.teletrust.de/it-sicherheit-in-der-hotellerie

<table>
<tr><th>Land</th><th>Beschreibung</th></tr>
<tr><td>
DE</td><td>
IT-Sicherheitsnavigator

Laufzeit:
Das Angebot steht seit 2011 zur Verfügung.

Ansatz:
Über die Website der Initiative *IT-Sicherheit in der Wirtschaft* können Interessierte mit Hilfe des IT-Sicherheitsnavigators eine Datenbank anhand von Filtern nach den gewünschten Angeboten durchsuchen. Derzeit sind 486 einzelne Angebote gelistet, die sich nach Bundesland, Sektor (Dienstleistung, Handel, Handwerk, Industrie, Andere) und Schwerpunkt (Cloud, Datenschutz, E-Business, Mobiles Arbeiten, Organisation, Rechtsfragen, Sichere Rechner und Netzwerke, Soziale Netzwerke) sowie nach Suchworten filtern lassen.

Kontakt:
Marco Schuldt
Bundesministerium für Wirtschaft und Energie
Villemombler Str. 76, 53123 Bonn
Tel: 0049 30 18615-3228 / E-Mail: marco.schuldt@bmwi.bund.de

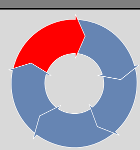
Webseite:
http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Angebote/navigator.html</td></tr>
<tr><td>
DE</td><td>
Erster Deutscher IT-Sicherheitspreis für kleine und mittelständische Unternehmen

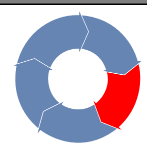
Laufzeit:
1. Mai 2012 bis 28. Februar 2013

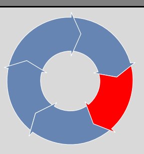
Ansatz:
Das BMWi lobte für besonders vorbildhafte Konzepte zur Informationssicherheit die bereits in KMU Anwendung finden, einen Preis für die betreffenden Unternehmen aus, der nach Begutachtung durch eine Jury im Rahmen der Verleihung des *IT-Sicherheitspreises* der *Horst Görtz-Stiftung* verliehen wurde.

Kontakt:
Dr. Michael Kreutzer
Technische Universität Darmstadt, Center for Advanced Security Research Darmstadt (CASED)
Mornewegstraße 32, 64293 Darmstadt
Tel: 0049 6151 16-6165 / E-Mail: michael.kreutzer@cased.de

Webseite:
http://it-sicherheitspreis.cased.de</td></tr>
</table>

Land	Beschreibung
 **DE**	 **IT-Sicherheitstag NRW** Diese Initiative wurde exemplarisch für die diversen *IT-Sicherheitstage* der Kammern ausgewählt. Dabei ist jedoch zu beachten, dass die Resonanz in den einzelnen Kammerbezirken unterschiedlich ausfällt. **Laufzeit:** Der Tag war von 2003 bis 2009 eine jährliche Großveranstaltung für mittelständische Unternehmen im Rahmen der Förderinitiative secu-re.it.nrw inklsive der Verleihung des *IT-Sicherheitspreises NRW*. Von 2010 bis 2012 wurde die Veranstaltung durch die IHK zu Köln, SIHK Hagen und IHK Bonn/Rhein-Sieg auf Basis einer Nachhaltigkeitsverein-barung mit dem Land NRW fortgeführt. **Ansatz:** Der *IT-Sicherheitstag* ist eine kostenpflichtige Messe mit Informations-angeboten in Form von Ausstellungsständen und Vorträgen. Aktuell ist die Veranstaltung auf 200 KMU ausgelegt, die 2013 die Angebote von 31 Partnern in Anspruch nehmen konnten. Die Themen der einzelnen Veranstaltungen sind nach Zielgruppen bzw. Inhalte geordnet (Basics, Experts, Institutionen, Initiativen und Projekte nach Zielgruppen) und werden in Abstimmung mit den 16 Koordinatoren in den einzelnen Kammern festgelegt. **Kontakt:** Dieter Schiefer IHK Köln Unter Sachsenhausen 10-26, 50667 Köln Tel: 0049 221 1640-520 / E-Mail: dieter.schiefer@koeln.ihk.de **Webseite:** http://www.it-sicherheitstag-nrw.de

Land	Beschreibung
 DE	**Kompetenzzentrum für IT-Sicherheit und Qualifizierte digitale Signatur der Handwerkskammer Rheinhessen (komzet@hwk)**  **Laufzeit:** 1. April 2006 bis 30. März 2009 **Ansatz:** Im Rahmen des durch das BMWi und das *Ministerium für Wirtschaft, Verkehr, Landwirtschaft und Weinbau Rheinland-Pfalz* geförderten Projekts führte das *komzet@hwk* kostenlose Lehrgänge für Inhaber und Mitarbeiter von Handwerksbetrieben im Kammerbezirk durch. Dabei wurden einzelne Lehrgänge gezielt für bestimmte Gewerke veranstaltet – z.B. Datenschutz bei Kfz-Werkstätten oder VoIP für Elektriker. Die Lehrgänge werden auch nach Auslaufen der Förderung angeboten, allerdings gegen eine geringe Gebühr, um die Präsenzquote zu erhöhen. Das Angebot *des komzet@hwk* umfasst darüber hinaus eine Beratung der Betriebe sowohl per Telefon und E-Mail als auch vor Ort, die nach Auslaufen der Förderung im Zuge der obligatorischen Betriebsberatung der Kammer weiterhin kostenlos geblieben ist. **Kontakt:** Jürgen Schüler Handwerkskammer Rheinhessen Dagobertstraße 2, 55116 Mainz Tel: 0049 6131 9992-61 / E-Mail: j.schueler@hwk.de **Webseite:** http://www.komzet-hwk.de

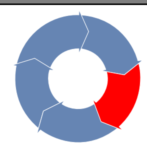
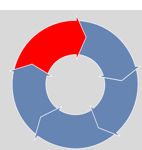
<table>
<tr><th>Land</th><th>Beschreibung</th></tr>
<tr><td>
DE</td><td>**nrw.units**


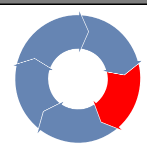
Laufzeit:
Juli 2012 bis November 2014

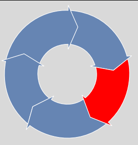
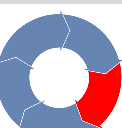
Ansatz:
Das Projekt, finanziert aus Mitteln des *Ministeriums für Wirtschaft, Energie, Industrie, Mittelstand und Handwerk des Landes Nordrhein-Westfalen* sowie des *Europäischen Fonds für regionale Entwicklung*, wird durch ein breites Netzwerk getragen, zu dem neben dem für das Projektmanagement zuständige *Horst Görtz Institut des Verbands der deutschen Internetwirtschaft e.V*. und der *networker NRW e.V*. als Partner sowie die Wirtschaftsförderung der Stadt Bochum und die IHK Mittleres Ruhrgebiet als Multiplikatoren und vor allem die Unternehmen und anderen Organisationen, die sich per „Letter of Intent“ zu einer Zusammenarbeit bereit erklärt haben, gehören. *nrw.units* bietet eine Plattform, auf der Unternehmen mit eigenen Studien, White Papers und Veranstaltungen ihre Expertise gezielt KMU vorstellen können und so die Spezialisierungsvorteile von kleinen und mittleren IT-Unternehmen herausgestellt und die Hemmschwelle für KMU, eine ansonsten mit Kosten verbundene Beratung zu einem Angebot in Anspruch zu nehmen, überwunden werden.

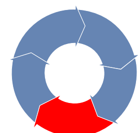
Kontakt:
Susanne Kersten
Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum, Universitätsstraße 150, 44780 Bochum, Raum ID 2 / 144
Tel: 0049 234 32-29599 / E-Mail: susanne.kersten@rub.de

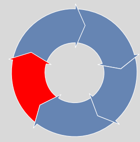
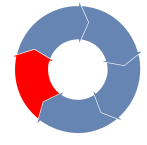
Webseite:
http://www.nrw-units.de</td></tr>
</table>

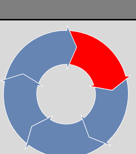
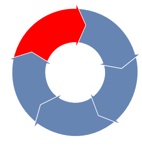
Land	Beschreibung
 **DE**	**PROF[IT]ABEL**  **Laufzeit:** Das Tool wurde 2013 fertiggestellt und befindet sich derzeit in der Markteinführungsphase. **Ansatz:** *PROF[IT]ABEL* ist ein durch das BMWi finanzierter und durch ein Konsortium aus der *Softwareforen Leipzig GmbH*, der *Goethe-Universität Frankfurt* sowie der *Universität Hamburg* erstellter webbasierter Assistent, mit dem die Wirtschaftlichkeit einer Investition in die IT-Sicherheit eines Unternehmens abgeschätzt werden kann. Liegen alle benötigten Informationen vor, benötigt man ca. 15 Minuten für die vollständige Bearbeitung. Dabei wird auf Basis der Nutzereingaben eine Abschätzung, wann eine konkrete IT-Sicherheitsmaßnahme eines Unternehmens voraussichtlich wirtschaftlich sein wird, erstellt. Zusätzlich sollen sich in Zukunft Unternehmen in eine Peer-Group einordnen können, sobald eine ausreichende Anzahl von Teilnehmern vorhanden ist. **Kontakt:** Marco Schuldt Bundesministerium für Wirtschaft und Energie Villemombler Str. 76, 53123 Bonn Tel: 0049 30 18615-3228 / E-Mail: marco.schuldt@bmwi.bund.de **Webseite:** https://profitabel.softwareforen.de
 **DE**	**Cloud- und Informationssicherheit – praktisch umgesetzt in KMU**  **Laufzeit:** Die Roadshow startete im Februar 2014. **Ansatz:** Der *Bayerische IT-Sicherheitscluster e.V*. stellt im Rahmen einer Roadshow in Zusammenarbeit mit den regionalen Industrie- und Handelskammern, die Räume zur Verfügung stellen und als Veranstalter auftreten, sowie weiterer wechselnder Partner auf zwei- bis dreistündigen Veranstaltungen die von den Mitgliedern des Clusters erarbeiteten Lösungen *ISIS12*, *ISA+* und *Certified Secure Cloud* vor. **Kontakt:** Sandra Wiesbeck Bayerischer IT-Sicherheitscluster e.V. Bruderwöhrdstr. 15 b, 93055 Regensburg Tel: 0049 941 604889-18 / E-Mail: sandra.wiesbeck@it-sec-cluster.de **Webseite:** http://www.it-sicherheit-bayern.de/IT-Sicherheitscluster

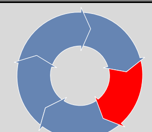
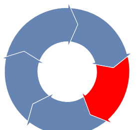
Land	Beschreibung
 DE	**SimoBIT – sichere Anwendung der mobilen Informationstechnik (IT) zur Wertschöpfungs-steigerung in Mittelstand und Verwaltung**  **Laufzeit:** 2007 bis 2011 **Ansatz:** Das Technologieprogramm *SimoBIT* förderte aus den Mitteln des BMWi in Höhe von 27,5 Mio. Euro einzelne Projekte von Unternehmen und Forschungseinrichtungen, die in etwa nochmals denselben Betrag aufbrachten. Insgesamt bestand das Programm aus vier Kompetenznetzwerken (Gesundheitswirtschaft, Maschinenbau, Öffentliche Verwaltung sowie Handwerk und kleine Unternehmen), in denen jeweils drei Leuchtturmprojekte durchgeführt wurden. Im Bereich KMU wurden so zwei Lösungen für Branchen (Handelsvertreter, Handwerker) und mit *ModiFrame* eine branchenunabhängige Entwicklungsplattform für KMU allgemein gefördert. Die einzelnen Projekte erhielten zudem eine Unterstützung durch die Begleitforschung, in deren Rahmen ein Konsortium unter Leitung der *WIK GmbH* Markt- und Wertschöpfungspotenzialstudien sowie technische Evaluationen der Projekte durchführte. Um zusammen mit anderen Stakeholdern mobilen Geschäftsanwendungen zum Durchbruch zu verhelfen, wurde zwischen dem BMWi und dem *Bundesverband Digitale Wirtschaft e.V*. die Vereinbarung getroffen, allen interessierten *SimoBIT*-Akteuren eine Plattform zu bieten, wozu sich im Februar 2011 in der Fachgruppe Mobile die *Unit Mobile Business Solutions* gründete. **Kontakt:** Dr. Christian Schmidt Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR) Linder Höhe, 51147 Köln Tel: 0049 2203 601-2801 / E-Mail: c.schmidt@dlr.de **Webseite:** http://www.simobit.de

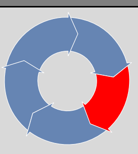
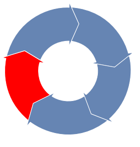
Land	Beschreibung
 **DE**	 **Trusted Cloud** **Laufzeit:** 2010 bis 2015 **Ansatz:** Das BMWi stellt Fördergelder von insgesamt 50 Mio. Euro für 14 Forschungs- und Entwicklungsprojekte zur Verfügung, an denen 38 Unternehmen, 26 wissenschaftliche Einrichtungen und fünf weitere Institutionen beteiligt sind. *Trusted Cloud* ist Bestandteil der IKT-Strategie *Deutschland Digital 2015* und der *Hightech-Strategie* der Bundesregierung. Das Programm soll die Vorteile von Cloud Computing anhand konkreter Pilotanwendungen verdeutlichen, von denen sich einige gezielt an KMU richten. Außerdem soll in einem Pilotprojekt KMU die Auswahl von Dienstleistern mit Hilfe einer Datenschutz-Zertifizierung von Cloud-Diensten erleichtert werden. **Kontakt:** Kompetenzzentrum Trusted Cloud c/o Innova Beratungsgesellschaft mbH Schopenhauerstraße 47 14129 Berlin Tel: 0049 30 3463 7590 / E-Mail: kompetenzzentrum@trusted-cloud.de **Webseite:** http://www.trusted-cloud.de
 **DE**	 **IT Security made in Germany** **Laufzeit:** Die Initiative wurde 2005 durch das BMI und das BMWi sowie Vertreter der deutschen IT-Sicherheits-wirtschaft initiiert und 2008 in einen eingetragenen Verein überführt. Seit 2011 werden die Aktivitäten unter dem Dach des Verbands *TeleTrusT e.V*. als eigenständige Arbeitsgruppe fortgeführt. **Ansatz:** Die Unternehmen, die den Anforderungen der Arbeitsgruppe genügen, dürfen mit dem Siegel *IT Security made in Germany* für ihre Sicherheits-produkte werben. Damit wird, auch wenn die Initiative in erster Linie deutschen Unternehmen die internationale Vermarktung eigener Lösungen erleichtern soll, zumindest indirekt das Angebot an Sicher-heitslösungen für heimische KMU gestärkt. **Kontakt:** Dr. Holger Mühlbauer TeleTrust – Bundesverband IT-Sicherheit e.V. Chausseestraße 17 10115 Berlin Tel: 0049 30 400 54 306 / E-Mail: holger.muehlbauer@teletrust.de **Website:** https://www.teletrust.de/itsmig/

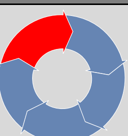
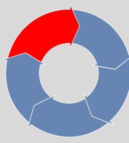
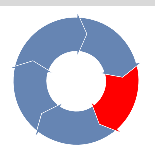
Land	Beschreibung
 **EE**	**Raising Public Awareness about the Information Society** **Laufzeit:** Seit 2007 **Ansatz:** Die Bewusstseinsförderungskampagne *Raising Public Awareness about the Information Society* wurde gemeinsam von der *Estonian Information Systems's Authority* RIA, dem Ministerium des Innern und dem Verteidigungsministerium entwickelt. Finanziert wird die Initiative durch den *Europäischen Fonds für regionale Entwicklung*. Im Zuge der Initiative finden mehrmals im Monat Schulungen zur sicheren Nutzung des Internets statt. Darüber hinaus werden ein bis zweimal im Jahr Informationskampagnen durchgeführt, die sich sowohl Plakaten als auch Social Media Plattformen bedient. **Kontakt:** Piret Aro RIA - Estonian Information System's Authority Rävala 5, Tallinn 15169 Estland Tel: +372 663 0298 / E-Mail: piret.aro@ria.ee **Webseite:** https://www.ria.ee/programme/
 **EE**	**Estonian Security Interoperability Framework**  **Laufzeit:** Im Jahr 2007 wurde eine erste Version veröffentlicht. 2011 wurde eine Version 2.0 finalisiert. **Ansatz:** Unter dem Eindruck des groß angelegten Angriffes auf die estnische IT-Infrastruktur im Jahr 2007 wurde *das Estonian Security Interoperability Framework* vom Ministerium für Wirtschaft und Kommunikation entwickelt. Das Framework beinhaltet Handlungsanweisungen für die Entwicklung sicherer IT-Schnittstellen für die Kommunikation mit staatlichen IT-Systemen. Zur Unterstützung werden Schulungen zur Erläuterung und Umsetzung angeboten. **Kontakt:** Aet Rahe Department of State Information Systems (Ministry of Economic Affairs and Communications) Harju 11, 15072 Tallinn Tel: +3726397640 / E-Mail: Aet.Rahe @ riso.ee **Webseite:** http://www.riso.ee/en/estonian-interoperability-framework

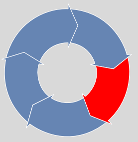
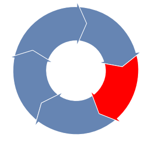
Land	Beschreibung
 **UK**	**Business Crime Reduction Center**  **Laufzeit:** Seit 2007 **Ansatz:** Das *Business Crime Reduction Center* wird zur Hälfte von dem *Europäischen Fonds für regionale Entwicklung* und zur anderen Hälfte von vier regionalen Polizeidirektionen finanziert. Unternehmen erhalten im Zuge der Initiative eine kostenlose IT-Sicherheitsberatung durch einen vom *Business Crime Reduction Center* zur Verfügung gestellten „Business Advisor". **Kontakt:** Lucy Straker Business Crime Reduction Center 3rd Floor, The Tower Furnival Square Sheffield, S1 4QL Tel: +44 114 275 1283 / E-Mail: lucy.straker@people-united.org **Webseite:** http://www.bcrc-uk.org/
 **UK**	**E-Crime Wales**  **Laufzeit:** Seit 2007 **Ansatz:** Die Initiative wird gemeinsam von der walisischen Regierung und den walisischen Polizeibehörden betrieben. Die Finanzierung erfolgt durch den *Europäischen Fonds für regionale Entwicklung*. Opfer von E-Crime sollen motiviert werden, etwaige Vorfälle an die entsprechenden Polizeistellen zu melden. Zusätzlich werden verschiedene Dokumente zur IT-Sicherheit kostenlos zum Download angeboten. Außerdem organisiert die Initiative einmal jährlich den *E-Crime Wales Summit.* **Kontakt:** Katherine Hibbert E-Crime Wales n/a Tel: +44 (0) 2920368244 / E-Mail: katherine.hibbert@wales.gsi.gov.uk **Webseite:** www.ecrimewales.com

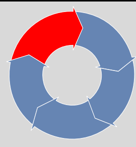
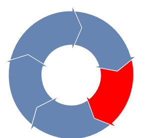
Land	Beschreibung
 **UK**	**E-Learning Platfom Bob's Business**  **Laufzeit:** Die Initiative wurde von 2005 bis 2007 durch das *Department for Business Innovation und Skills* sowie die *Mid Yorkshire Chamber of Commerce and Industry* betrieben. 2007 wurde das Projekt in eine GmbH überführt und trägt sich seitdem selbst. **Ansatz:** *Bob's Business* bietet E-Learning Einheiten zu verschiedenen Themen an. Diese sind in Cartoon-Form gehalten, um so bei den Nutzern eine höhere Einprägsamkeit zu erzeugen. Unternehmen, die *Bob's Business* nutzen, müssen eine jährliche Gebühr entrichten. Die Initiative soll Unternehmen in die Lage versetzen, Standards wie ISO 27001 einzuführen, was insbesondere KMU ansonsten schwer fiele. **Kontakt:** Melanie Oldham Bob's Business Digital Media Centre, County Way, Barnsley, S702JW Tel: +44 (0)1226 447 225 / E-Mail: melanie@bobs-business.co.uk **Webseite:** http://bobsbusiness.co.uk/
 **UK**	**Get Safe Online**  **Laufzeit:** Seit 2005 **Ansatz:** Verschiedene Akteure wie z.B. *Microsoft, Bob's Business, E-Crime Wales* oder das *Department for Business Innovation and Skills* unterstützen die Initiative mit vier Partnerschaftsmodellen. In erster Linie werden durch diese Bewusstseinsförderungskampagne Informationen zur Informationssicherheit bereitgestellt und auf andere Initiativen verwiesen. *Get Safe Online* stellt so mittlerweile einen zentralen Anlaufpunkt beim Thema Informationssicherheit in Großbritannien dar. **Kontakt:** Tony Neate Get Safe Online Clifton House, Four Elms Road, Cardiff, CF24 1LE Tel: +44 2070256662 / E-Mail: press@getsafeonline.org **Webseite:** https://www.getsafeonline.org/

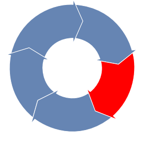
Land	Beschreibung
 UK	**Innovation Vouchers for Cyber Security**  **Laufzeit:** Die Initiative läuft seit 2007. Das Budget ist mindestens bis 2015 vorgesehen. Sollte die Finanzierung verlängert werden, soll auch die Initiative fortgesetzt werden. **Ansatz:** Die Initiative wird vom *Department for Business Innovation and Skills* finanziert und vom *Technology Strategy Board* betrieben. Circa 100 Unternehmen erhalten pro Quartal mittels eines Losverfahrens Zugang zu einem Gutschein in Höhe von 5000 Pfund für eine Beratung durch einen Cybersicherheitsexperten. Die Experten müssen ihre Eignung beim Träger zuvor nachweisen. **Kontakt:** David Golding The Technology Strategy Board North Star House North Star Avenue, Swindon SN2 1UE Tel: +44 1793 442762 / E-Mail: david.golding@tsb.gov.uk **Webseite:** https://vouchers.innovateuk.org/cyber-security
 NL	**Bescherm je bedrijf**  **Laufzeit:** Die Initiative existiert bereits seit November 2011. Das aktuelle Design sowie die aktuellen Funktionen wurden jedoch erst ein Jahr später im November 2012 veröffentlicht. **Ansatz:** Auf der Homepage von *Bescherm je bedrijf* können sich KMU allgemeines Informationsmaterial zum Thema Informationssicherheit herunterladen. Der *Stappenplan*, eine Roadmap zu mehr Informationssicherheit, stellt im Zusammenspiel mit einem *Quickscan* KMU individualisierte Handlungsempfehlungen zur Verfügung. **Kontakt:** Bart Pegge Nederland ICT Pompmolenlaan 7 3447 GK Woerden Tel: 0031 348 49 36 51 / E-Mail: bart.pegge@nederlandict.nl **Webseite:** www.beschermjebedrijf.nl

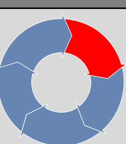
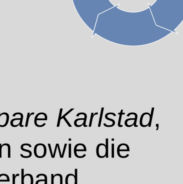
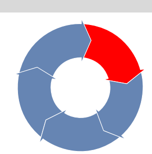
Land	Beschreibung
  NL	**Cyberrad**  **Laufzeit:** Das *Cyberrad* wurde im Rahmen der Veranstaltung *Risiko Cybercrime for KMU* am 11. März 2014 vorgestellt. **Ansatz:** Das *Cyberrad* wurde vom Verband niederländischer KMU, dem MKB, zusammen mit der *Technical Association for Applied Sciences* TNO gemeinsam finanziert und von letzterer entwickelt Das *Cyberrad* ist ein Tool auf der Website *www.stopcybercrime.nu*, durch das Unternehmen auf ihre Branche zugeschnittene Informationen zu Cyberbedrohungen erhalten. **Kontakt:** Suzanne Rijnbergen TNO Innovation for Life Oude Waalsdorpeweg 63 NL-2597 AK The Hague Tel: 0031 88 866 56 34 / E-Mail: suzanne.rijnbergen@tno.nl **Webseite:** http://www.stopcybercrime.nu/1444/cyberrad-risico-cybercrime-per-sector.htm
 NL	**Hulpknop**  **Laufzeit:** Seit Dezember 2013 **Ansatz:** Der *Hulpknop* wurde vom Justizministerium, dem MKB sowie *Digibewust* gemeinsam entwickelt. Ein visuell dargestellter Notfallknopf auf der *www.stopcybercrime.nu* Website führt Nutzer zu einer Auswahl, mit der Unternehmen den sie betreffenden Cybervorfall auswählen können. Anschließend werden ihnen Handlungsempfehlungen an die Hand gegeben. **Kontakt:** MKB Servicedesk Radonweg 7 NL 3542 Utrecht E-Mail: info@mkbservicedesk.nl **Webseite:** http://hulpknop.stopcybercrime.nu/

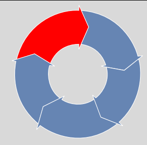
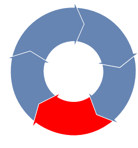
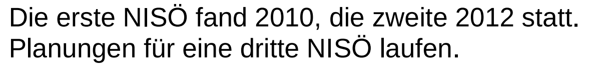
Land	Beschreibung
 NL	**Risiko Cybercrime for KMU**   **Laufzeit:** *Risiko Cybercrime for KMU* ist eine eintägige eranstaltung, die einmalig am 11. März 2014 durchgeführt wurde. **Ansatz:** Zu der Informationsveranstaltung zum Thema Cyberkriminalität wurden Vertreter verschiedener niederländischer Fachverbände eingeladen, die die dort gesammelten Erkenntnisse an ihre Mitglieder weitertragen sollten. Im Zuge der Veranstaltung wurde auch das *Cyberrad* vorgestellt. **Kontakt:** Suzanne Rijnbergen TNO Innovation for Life Oude Waalsdorpeweg 63 NL-2597 AK The Hague Tel: 0031 88 866 56 34 / E-Mail: suzanne.rijnbergen@tno.nl **Webseite:** https://www.tno.nl/content.cfm?context=uitgelicht&content=uitgelicht_evenement&laag1=1229&item_id=892
 NL	**Cyberscan**  **Laufzeit:** Seit 2013 **Ansatz:** Auf der Website *www.stopcybercrime.nu* wird mit dem *Cyberscan* ein Tool angeboten, dass dem bei *Bescherm je bedrijf* angebotenen *Quickscan* entspricht. Anhand von 10 Fragen werden Risiken identifiziert und Handlungsempfehlungen abgeleitet. **Kontakt:** MKB Servicedesk Radonweg 7 NL 3542 Utrecht E-Mail: info@mkbservicedesk.nl **Webseite:** http://www.stopcybercrime.nu/

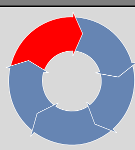
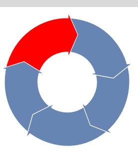
Land	Beschreibung
 **NL**	**Waarschuwingsdienst.nl**  **Laufzeit:** Seit 2013. **Ansatz:** Der *Waarschuwingsdienst* wurde vom zum Justizministerium gehörenden *National Cyber Security Centrum* entwickelt und betrieben. Der Waarschuwingsdienst stellt KMU sowie Privatpersonen mittels Email und SMS sowie auf der Website Informationen zum aktuellen Bedrohungen und Sicherheitslücken zur Verfügung. **Kontakt:** National Cyber Security Centrum Turfmarkt 147 NL 2511 DP Den Haag E-Mail: info@ncsc.nl **Webseite:** https://www.waarschuwingsdienst.nl/English
 **AT**	**IKT Sicherheitsportal**  **Laufzeit:** Seit 2013 **Ansatz:** Das *IKT Sicherheitsportal* wurde vom *Bundesministerium für Finanzen*, dem *Bundeskanzleramt* und dem *Zentrum für sichere Informationstechnologie* A-SIT entwickelt. Stellt auf seiner Website zielgruppenspezifische Handlungsempfehlungen zur Verfügung. Der Inhalt des österreichischen *Informationssicherheitshandbuchs* ist ebenfalls in das Informationsmaterial auf der Website integriert. **Kontakt:** Manfred Holzbach A-Sit - Zentrum für sichere Informationstechnologie Seidlgasse 22 / Top 9, 1030 Wien Tel: +43 1 503 19 63 - 30 / E-Mail: manfred.holzbach@a-sit.at **Webseite:** www.onlinesicherheit.gv.at

Land	Beschreibung
  **AT**	 **Roadshow "Schutz vor Cyberkriminalität"** **Laufzeit:** Seit Oktober 2013 **Ansatz:** Die Initiative wird vom *Bundesministerium für Inneres*, der *Polizei Österreich*, der *Wirtschaftskammer Österreich* sowie dem *Kuratorium Sicheres Österreich* entwickelt. Bundesweit werden dabei Informationsveranstaltungen von Vertretern des KSÖ durchgeführt. Ende 2013 hatten bereits über 100 Veranstaltungen stattgefunden. **Kontakt:** Christian Kunstmann Kuratorium Sicheres Österreich Herrengasse 7, Postfach 100, 1014 Wien Tel: +43 1 53126-2236 oder 2395 / E-Mail: office@kuratorium-sicheres-oesterreich.at **Webseite:** www.cybersicherheit.at
 **AT**	 **Schecks für Sicherheitschecks** **Laufzeit:** Die Initiative wurde von 2005 bis 2007 durchgeführt. Nach Beendigung der Finanzierung durch das *Bundesministerium für Wissenschaft, Forschung und Wirtschaft* wurde die Initiative auch beendet. **Ansatz:** Im Rahmen der Initiative wurden Gutscheine für die Inanspruchnahme einer individuellen Beratung von einem halben Tag ausgegeben. Die Beratung wurde durch Vertreter der *IT-Security Expert Group* der WKO durchgeführt. **Kontakt:** Mag. Bogendorfer KommR Prof. Pollirer Wirtschaftskammer Österreich Wiedner Hauptstraße 63, 1045 Wien Tel: +43 (0)5 90 900 3175 / E-Mail: Rene.Bogendorfer@wko.at **Webseite:** www.wko.at

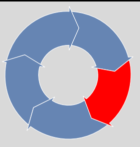
Land	Beschreibung
 **AT**	**Sicher im Internet**  **Laufzeit:** Seit 2005 **Ansatz:** Die Initiative wurde von *Microsoft Österreich* initiiert und vom *Bundesministerium für Inneres* sowie der *Wirtschaftskammer Österreich* unterstützt. Auf der Website können Unternehmen anhand kostenfreier Checklisten den Stand Ihrer Informationssicherheit evaluieren. **Kontakt:** Dr. Gerhard Laga Wirtschaftskammer Österreich Wiedner Hauptstraße 63, 1045 Wien Tel: +43 (0)5 90 900 4203 / E-Mail: Gerhard.Laga@wko.at **Webseite:** www.sicher-im-internet.at
 **AT**	**it-safe.at**  **Laufzeit:** Seit 2004 **Ansatz:** Die Initiative wurde von der *Wirtschaftskammer Österreich* entwickelt. Auf der Website der Initiative wird kostenloses Informationsmaterial zur Verfügung gestellt. Im Zuge der Initiative wurden 2 IT-Sicherheitshandbücher entwickelt. Eines adressiert Mitarbeiter, das andere Geschäftsführer von KMU. Die Handbücher wurden bereits 50.000 Mal als Printmedium angefordert. Die Zahl der Downloads bleibt hier unberücksichtigt. **Kontakt:** Mag. Rene Bogendorfer KommR Prof. Hans-Jürgen Pollirer Wirtschaftskammer Österreich (Bundessparte Information & Consulting) Wiedner Hauptstraße 63, 1045 Wien Tel: +43 (0)5 90 900 3175 / E-Mail: Rene.Bogendorfer@wko.at **Webseite:** www.it-safe.at

Land	Beschreibung
 **SE**	 **ISIS (IT Sicherheit in Skandinavien)** **Laufzeit:** Januar 2013 bis August 2014  **Ansatz:** Die Initiative wurde von der schwedischen Stiftung *Compare Karlstad*, der mehr als 100 Unternehmen, öffentliche Einrichtungen sowie die Karlstad Universität angeören und dem norwegischen Verband *Kunnskapsbyen Lillestrom* entwickelt und durchgeführt. Im Zuge der Initiative werden verschiedene Seminare und Konferenzen abgehalten, so zum Beispiel „Internet und Sicherheit“ oder „Security Divas“. **Kontakt:** Mikael Lundström Stiftelsen Compare Karlstad Vaxnasgatan 2 653 40 Karlstad Tel: / E-Mail: mikael.lundstrom@comparse.es **Webseite:** http://www.compare.se/projekt/isis
 **SE**	 **1-tägige Kurse für KMU** **Laufzeit:** Seit 1996 **Ansatz:** Die Kurse werden von der *Königlich Technichen Hochschule Stockholm* durchgeführt. Es werden Kurse für bis zu 25 Personen angeboten, wobei der Preis individuell verhandelt wird. Zielgruppe sind in erster Linie Vertreter von KMU, die über keine eigene IT-Abteilung verfügen. Behandelt werden grundlegende Themen zur IT-Sicherheit **Kontakt:** L.O. Stromberg KTH - Royal Institute of Technology Valhallavägen 79 100 44 Stockholm Sweden Tel: 0046 70 144 3400 / E-Mail: los@kth.se **Webseite:** http://www.edab.kth.se/oppen-utbildning/informationssakerhet-1.69164

Land	Beschreibung
 **SE**	**Programmes to support IT-Security**  **Laufzeit:** Die Initiative ist noch in Planung. Sie soll aber dieses Jahr noch gestartet werden. **Ansatz:** Die Initiative wird von der *schwedischen Civil Contingencies Agency* MSB angeleitet. Geplant ist, im Dialog mit schwedischen KMU entsprechende Angebote zu entwickeln. Es sollen aufbauend auf dem bisherigen Programm des MSB Schulungen und Workshops angeboten werden. **Kontakt:** Fia Ewald MSB (Swedish Civil Contingencies Agency) SE-651 81 KARLSTAD Sweden Tel: 46 (0) 771-240 240 / E-Mail: Fia.Ewald@msb.se **Webseite:** Noch nicht vorhanden
 **SE**	**National Cyber Security Excercise (NISÖ 2012)**  **Laufzeit:**  Die erste NISÖ fand 2010, die zweite 2012 statt. Planungen für eine dritte NISÖ laufen. **Ansatz:** Die MSB führte mit 17 beteiligten Organisationen und Unternehmen die NISÖ durch um Kooperation und Koordination zu verbessern. Die Initiative zielt auf die kritische Infrastruktur, zu der laut eines Experteninterviews in Schweden auch KMU gehören. **Kontakt:** Fia Ewald MSB (Swedish Civil Contingencies Agency) SE-651 81 KARLSTAD Sweden Tel: 46 (0) 771-240 240 / E-Mail: Fia.Ewald@msb.se **Webseite:** http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/presentations/roger-holfeldt-msb-sweden-the-national-cyber.pdf

Land	Beschreibung
  **SE**	**Infoportal**  **Laufzeit:** Das Infoportal der *Post and Telecom Authority* PTS geht dieses Jahr an das MSB über. Die Initiative lief von 2005 bis 2014. **Ansatz:** Auf der Website der PTS wird eine große Bandbreite an Informationen zur Informationssicherheit zur Verfügung gestellt. Außerdem wurde zur Verbreitung ein Youtube-Kanal genutzt. **Kontakt:** Erika Hersaeus PTS Valhallavägen 117 115 31 Stockholm Tel: 0041 70 760 56 34 / E-Mail: Erika.Hersaeus@pts.se **Webseite:** http://www.pts.se/en-GB/Industry/Internet/
 **SE**	**Info-Tour**  **Laufzeit:**  Die Initiative wurde von 2007 bis 2008 durchgeführt. Aus Gründen der mangelnden Effektivität wurde sie jedoch nach zwei Jahren bereits wieder eingestellt. **Ansatz:** Die PTS führte gemeinsam mit Unternehmen aus dem IT-Sektor wie *Microsoft* und *Symantec* eine Roadshow durch. Die Kampagne tourte zweimal im Jahr im Frühling und im Herbst durch schwedische Groß-städte. Angeboten wurden Infoveranstaltungen zum Thema IT-Sicherheit. **Kontakt:** Erika Hersaeus PTS Valhallavägen 117 115 31 Stockholm Tel: 0041 70 760 56 34 / E-Mail: Erika.Hersaeus@pts.se **Webseite:** Nicht vorhanden

<table>
<tr><th>Land</th><th>Beschreibung</th></tr>
<tr><td>

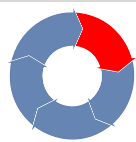
ES</td><td>Procedures and Documents


Laufzeit:
Seit Juni 2013

Ansatz:
Die Initiative wird vom Industrial Cybersecurity Center (CCI) durchgeführt. Die Angebote können sowohl von Privatpersonen als auch von Unternehmen mittels verschiedener Mitgliedschaftsmodelle wahrgenommen werden. Das CCI hat einen Mangel an spanisch sprachiger Dokumentation zum Thema IT-Sicherheit identifiziert. Es gibt verschiedene kostenpflichtige und kostenfreie Angebote an Verfahrensanweisungen und „Best Practices“. Die frei erhältliche Cybersecurity Roadmap wurde bereits 30.000 mal heruntergeladen. Die Reichweite der Initiative erstreckt sich nicht nur auf Spanien sondern den gesamten spanisch sprachigen Raum.

Kontakt:
Ignacio Paredes
Industrial Cybersecurity Center
Centro de Ciberseguridad Industrial
Calle Maiquez 18
E-28009, Madrid
Tel: 0034 6477 23708 / E-Mail: Ignacio.Paredes@cci-es.org

Webseite:
http://www.cci-es.org/web/cci/formacion</td></tr>
<tr><td>

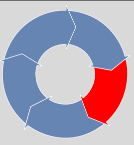
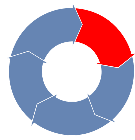
ES</td><td>Training


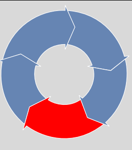
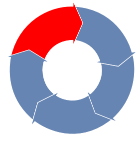
Laufzeit:
Seit Juni 2013

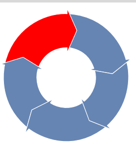
Ansatz:
Vom CCI werden neben den Procedures and Documents auch Trainings angeboten. Diese sind für Mitglieder und Nichtmitglieder unterschiedlich zugänglich und mit verschiedenen Kosten verbunden. Der Umfang der Trainings variiert von einer Stunde bis hin zu einer Woche.

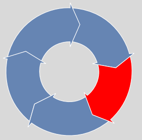
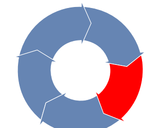
Kontakt:
Ignacio Paredes
Industrial Cybersecurity Center
Centro de Ciberseguridad Industrial
Calle Maiquez 18
E-28009, Madrid
Tel: 0034 6477 23708 / E-Mail: Ignacio.Paredes@cci-es.org

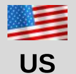
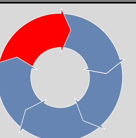
Webseite:
http://www.cci-es.org/web/cci/formacion</td></tr>
</table>

Land	Beschreibung
  **ES**	 **INTECO-Cert** **Laufzeit:** Seit 2006 **Ansatz:** Das *Instituto Nacional de Tecnologías de la Comunicación* (INTECO) betreibt seit seiner Gründung 2006 das *INTECO-Cert*. Über das *INTECO-Cert* werden Informationen zu aktuellen Cyberbedrohungen sowie zu geeigneten Schutzmaßnahmen angeboten. Darüber hinaus gibt es Zugang zu Beratungen zum Management von Cybervorfällen und zu Rechtsberatung. **Kontakt:** Jorge Chinea Lopéz INTECO Avenida José Aguado 42 Edificio INTECO 24005 León Tel: 0034 987 877 189 / E-Mail: jorge.chinea@inteco.es **Webseite:** https://www.inteco.es/Training/SMEs/
 **ES**	 **Awareness Raising, Education and Training Program** **Laufzeit:** 2013 bis 2015 **Ansatz:** Neben seinem *INTECO-Cert* bietet INTECO über diese Initiative KMU eine große Bandbreite an Informationen und Angeboten. So existieren ein Blog mit relevanten Neuigkeiten, ein Service wo komplexe IT-Sachverhalte in verständlicher Sprache dargestellt sind, ein *Security Kit*, bei dem es sich um ein Set von Lernangeboten handelt, weitere Online-Lernangebote sowie ein Tool zur Selbstdiagnose des Standes der IT-Sicherheit. **Kontakt:** Jorge Chinea Lopéz INTECO Avenida José Aguado 42 Edificio INTECO 24005 León Tel: 0034 987 877 189 / E-Mail: jorge.chinea@inteco.es **Webseite:** https://www.inteco.es/Training/SMEs/

Land	Beschreibung
  ES	**Summer Excercise 2013**  **Laufzeit:** Seit Januar 2013 **Ansatz:** Vom *ISMS Forum Spain*, INTECO sowie weiteren Unternehmen wird ein umfangreicher Penetrationstest der IT-Infrastruktur von Großunternehmen vorgenommen. Diese autorisierten Cyberangriffe beinhalten außerdem umfangreiche Überwachung sowie einen Abschlussreport inklusive eines Benchmarks. Bis dato nehmen lediglich Unternehmen des ersten spanischen Aktienindexes teil, wobei es Überlegungen gibt die Initiative auf KMU auszuweiten. **Kontakt:** Gianluca d'Antonio ISMS Forum Spain ISMS Forum Spain Castelló, 24, 5 D. Escalera 1 28001 Madrid Tel: 0034 911 861 350 / E-Mail: GDAntonio@fcc.es **Webseite:** Nicht vorhanden
  ES	**Voice of the Industry**  **Laufzeit:** Seit 2013 **Ansatz:** Bei der vom *Industrial Cyber Security Center* CCI durchgeführten halbtägigen Konferenz *Voice of the Industry* geht es um Cybersicherheit. Ziel ist es unter anderem den Markt für Cybersicherheitsprodukte und Dienstleistungen zu vergrößern. **Kontakt:** Ignacio Paredes Industrial Cybersecurity Center Centro de Ciberseguridad Industrial Calle Maiquez 18 E-28009, Madrid Tel: 0034 6477 23708 / E-Mail: Ignacio.Paredes@cci-es.org **Webseite:** http://www.cci-es.org/web/cci/detalle-evento/-/journal_content/56/10694/57072

Land	Beschreibung
 **US**	**CISO in residence Programm** **Laufzeit:** Seit 2014 **Ansatz:** Die Initiative wird vom *Howard Tech Council*, einem Teil der *Howard County Economic Development Authority* durchgeführt. Die hier organisierten Unternehmen stellen KMU pro Bono einen virtuellen CISO zur Verfügung. **Kontakt:** Terry Owens Howard County Economic Development Authority (HCEDA) 6751 Columbia Gateway Dr, Suite 500 Columbia, MD 21046 United States Tel: 001 410 313 6500 / E-Mail: towens@hceda.org **Webseite:** Eigene Homepage nicht vorhanden
 **US**	**Cybersecurity for Small Businesses**  **Laufzeit:** Seit Oktober 2013 **Ansatz:** Die Initiative wird von der *U.S. Small Business Administration* (SBA) durchgeführt. KMU wird hier ein 30 minütiger Webcast angeboten, der allgemeine Informationen und Handlungsempfehlungen zu Cybersicherheit beinhaltet. Als zusätzlichen Anreiz können sich Absolventen des Webcasts ein individualisiertes Zertifikat herunterladen **Kontakt:** Jane Boorman U.S: Small Business Administration (SBA) Washington Office Center 409 3rd Street, S.W. Suite 6400 Washington, D.C. 20416 United States Tel: 001 202 205 7411 / E-Mail: jane.boorman@sba.gov **Webseite:** http://www.sba.gov/content/new-online-security-course-available-small-business-owners

Land	Beschreibung
 **US**	 **Securing our eCity** **Laufzeit**: Seit 2011 **Ansatz:** Federführend bei dieser Initiative für die Stadt San Diego ist die von dem slowakischen Sicherheitssoftwareunternehmen *ESET LLC* gegründete *ESET Foundation*, an der sich verschiedene andere Akteure als „Donors“ und „Partners“ beteiligen, unter anderem die städtische Polizei. Es werden für verschiedene Rezipienten 60-75 minütige Workshops durchgeführt, deren Inhalte im Vorfeld abgestimmt werden. **Kontakt:** Liz Fraumann ESET Foundation 610 West Ash Street Suite 1700-1 San Diego, California, 92101-3300 Tel: 001 619 630 2445 / E-Mail: liz.fraumann@esetfoundation.org **Webseite:** http://securingourecity.org/request-a-workshop
 **US**	 **Small Biz Cyber Planner 2.0** **Laufzeit:** Die erste Ausgabe des *Small Biz Cyber Planner* lief von Oktober 2011 bis Oktober 2012. Seitdem gibt es den *Small Biz Cyber Planner 2.0*. **Ansatz:** Die *Federal Communications Commission* (FCC) hat die Initiative entwickelt. KMU können durch das Eintragen der Unternehmensspezifika in einem Webtool einen individualisierten Plan zur Verbesserung der Cybersicherheit erhalten, der bei Auswahl sämtlicher Variablen maximal 51 Seiten enthält. **Kontakt:** David Bray Federal Communications Commission 445 12th Street SW, Washington DC 20554 Tel: 001 888 835 5322 / E-Mail: David.Bray@fcc.gov **Webseite:** http://www.fcc.gov/cyberforsmallbiz

Land	Beschreibung
 **US**	 **Small Business Corner (SBC)** **Laufzeit:** Die Planung der Initiative wurde 2000 begonnen und 2001 mit der Durchführung von Pilotworkshops begonnen. 2002 wurde die Initiative in den Regelbetrieb überführt. **Ansatz:** Die Initiative wird durch ein sogenanntes *„Interagency-Agreement“* vom *National Institute of Standards and Technology* (NIST), der *U.S. Small Business Administration* (SBA) und dem *Federal Bureau of Investigation* (FBI) durchgeführt. Im Zuge der Initiative werden bundesweit Workshops durchgeführt. Es wird versucht, die Veranstaltungen breit über das Land zu streuen, allerdings können Kongressabgeordnete in Washington Workshops für ihren Wahlkreis anfragen. **Kontakt:** Richard Kissel NIST (National Institute of Standards and Technology) 100 Bureau Drive M/S 8930 Gaithersburg, MD 20899-8930 Tel: 001 301 975 5017 / E-Mail: richard.kissel@nist.gov **Webseite:** http://csrc.nist.gov/groups/SMA/sbc/workshops.html

7 Literaturverzeichnis

Albrechtsen, Eirik (2007): A qualitative study of users' view on information security. In: *Computers & Security* 26, S. 276–289.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) (2013): Annual Report 2013.

Barney, Jay B. (1991): Firm Resources and Sustained Competitive Advantage. In: *Journal of Management* 17 (1), S. 99–120.

Brandl, Stefan; Scharioth, Sven (2013): IT-Sicherheitslage im Mittelstand 2013. Deutschland sicher im Netz e.V. (DsiN). Berlin.

Büllingen, Franz; Hillebrand, Annette (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Bundesministerium für Wirtschaft und Technologie (BMWi). Berlin.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2008): BSI-Standard 100-1. Managementsysteme für Informationssicherheit (ISMS). Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2011a): Die Lage der IT-Sicherheit in Deutschland 2011. Bonn.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2011b): Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Bonn.

Bundeskanzleramt Österreich (2012): Nationale IKT-Sicherheits-Strategie Österreich. Wien.

Bundeskanzleramt Österreich (2013a): Österreichische Strategie für Cyber Sicherheit. Wien.

Bundeskanzleramt Österreich (2013b): Österreichisches Informationssicherheitshandbuch. Version 3.1.5. Wien.

Bundesministerium des Innern (2011): Cyber-Sicherheitsstrategie für Deutschland. Berlin.

Bundesministerium für Inneres Österreich (2013): Die Entwicklung der Kriminalität in Österreich 2013. Kurzinformation.

Bundesverband mittelständische Wirtschaft (2013): Erfolgsfaktor IT-Sicherheit. Vom Mittelstand für den Mittelstand. Berlin.

Cabinet Office (2010): A Strong Britain in an Age of Uncertainty: The National Security Strategy. Online verfügbar unter https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty.

Cabinet Office (2011): The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world. London.

Cabinet Office (2013): Progress Against the Objectives of the National Cyber Security Strategy - December 2013.

Chia, Pauline A.; Maynard, Sean B.; Ruighaver, Anthonie B. (2002): Understanding organizational security culture. In: Proceedings of PACIS2002. Tokyo. Association for Information Systems.

Cisco Austria (Hg.) (2012): IT-Sicherheit in Österreichs Unternehmen.

Computer Emergency Response Team Austria (CERT.at) (2013): Bericht Internet-Sicherheit Österreich 2013.

Computerwelt.at (03.03.2014): WKO-Studie: KMU mit Nachholbedarf bei Sicherheitsvorkehrungen. Online verfügbar unter http://www.computerwelt.at/news/technologie-strategie/security/detail/artikel/101637-wko-studie-kmu-mit-nachholbedarf-bei-sicherheitsvorkehrungen/.

CPNI.NL (2013): From Learning by Doing to Leading by Doing. Seven years of public private partnership Seven years pf public private partenrship in the National Infrastructure against Cybercrime Cybercrime.

Department for Business, Innovation and Skills (BIS) (2014a): Cyber Essentials Scheme. Proposed assurance framework. London.

Department for Business, Innovation and Skills (BIS) (2014b): Information Security Breaches Survey 2014. Technical Report.

Der Standard (Hg.) (2013): Industrie startet Forum zum Schutz vor Cyber-Attacken. Online verfügbar unter http://derstandard.at/1369264118799/Industrie-startet-Forum-zum-Schutz-vor-Cyber-Attacken, zuletzt aktualisiert am 23.05.2013, zuletzt geprüft am 06.05.2014.

Detert, James A.; Schroeder, Roger G.; Mauriel, Jojn J. (2000): A Framework for linking culture and improvement initiatives in organizations. In: *Academy of Management Review* 25 (4), S. 850–863.

Duscha, Andreas; Klees, Maria; Weisser, Reinhard (2011): Netz- und Informationssicherheit in Unternehmen 2011. Netzwerk Elektronischer Geschäftsverkehr. Köln.

Eichfelder, Sebastian; Schorn, Michael (2012): Tax Compliance Costs: A Business-Administration Perspective. In: *FinanzArchiv / Public Finance Analysis* 68 (2), S. 191–230.

Enterprising Barnsley (17.12.2013): Bob helps build the business for Barnsley firm. Online verfügbar unter http://www.enterprisingbarnsley.co.uk/news/bob-helps-build-the-business-for-barnsley-firm, zuletzt geprüft am 21.05.2014.

Europäische Kommission (2006): Die neue KMU-Definition. Benutzerhandbuch und Mustererklärung. Luxemburg: Amt für Veröffentlichungen der Europäischen Union.

Europäische Kommission (2010): Die Mehrwertsteuer in der Europäischen Gemeinschaft. MwSt-Vorschriften in den Mitgliedstaaten Informationen für Behörden, Unternehmer, Informationsnetze usw. Brüssel (TAXUD/C/1).

Europäische Kommission (2013a): SBA Fact Sheet. Spain.

Europäische Kommission (2013b): SBA Fact Sheet. The Netherlands.

Europäische Kommission (2013c): SBA Fact Sheet. Austria.

Europäische Kommission (2013d): SBA Fact Sheet. Estonia.

Europäische Kommission (2013e): SBA Fact Sheet. United Kingdom.

Europäische Kommission (2013f): SBA Fact Sheet. Sweden.

European Network and Information Security Agency (ENISA) (2011a): Estonia Country Report. Heraklion.

European Network and Information Security Agency (ENISA) (2011b): Germany Country Report. Heraklion.

European Network and Information Security Agency (ENISA) (2011c): Sweden Country Report. Heraklion.

European Network and Information Security Agency (ENISA) (2011d): United Kingdom Country Report.

European Network and Information Security Agency (ENISA) (2012): National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyber-space.

Eurostat (08.02.2011): Safer Internet Day. Fast ein Drittel der Internetnutzer in der EU27 war von einem Computervirus betroffen.

Eurostat (18.12.2013): Internetzugang und Nutzung in 2013. Mehr als 60% der Personen in der EU28 nutzen täglich das Internet.

Germany Trade & Invest (2014): Investitionsklima und -risiken.

Geschonneck, Alexander; Fritzsche, Thomas (2013): e-Crime. Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz. KPMG.

Ghobakhloo, Morteza; Sabouri, Mohammad S.; Hong, Tang Sai; Zulkifli, Norzima (2011): Information Technology Adoption in Small and Medium-sized Enterprises; An Appraisal of Two Decades Literature. In: *Interdisciplinary Journal of Research in Business* 1 (7), S. 53–80.

Giannakouris, Konstantinos; Smihily, Maria (2011): ICT security in enterprises, 2010. Statistics in focus 7/2011. Eurostat.

Giannakouris, Konstantinos; Smihily, Maria (2012): ICT usage in enterprises 2012. Statistics in focus 46/2012. Eurostat.

Gillies, Alan (2011): Improving the quality of information security management systems with ISO27000. In: *The TQM Journal* 23 (4), S. 367–376.

Government Communications Headquarters (GCHQ) (2012): 10 Steps to cyber security. Online verfügbar unter https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.

Government Communications Headquarters (GCHQ) (13.08.2013): Cyber Incident Response Scheme Launched. Online verfügbar unter http://www.gchq.gov.uk/press_and_media/ press_releases/Pages/CIR-Scheme-Launched.aspx.

Gupta, Atul; Hammond, Rex (2005): Information systems security issues and decisions for small businesses: An empirical examination. In: *Information Management & Computer Security* 13 (4), S. 297–310.

Harindranath, G.; Dyerson, R.; Barnes, D. (2008): ICT Adoption and Use in UK SMEs: a Failure of Initiatives? In: *The Electronic Journal Information Systems Evaluation* 11 (2), S. 91–96. Online verfügbar unter http://www.ejise.com/volume11/issue2#, zuletzt geprüft am 18.10.2013.

Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2008): Study on security incidents and needs in Spanish small and medium-sized enterprises. Madrid.

Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2010): Executive summary of the Study on security and e-trust in the small and micro Spanish companies. Madrid.

Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2012a): Executive summary of the Study on information security and business continuity of Spanish enterprises. Madrid.

Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2012b): Executive summary of the Study on information security and business continuity of Spanish enterprises. Madrid.

Internet Security Alliance (2013): The Advanced Persistent Threat. Practical Controls That Small and Medium-Sized Business Leaders Should Consider Implementing.

Jolie O'Dell (2012): Guess who’s winning the brains race, with 100% of first graders learning to code? Venturebeat. Online verfügbar unter http://venturebeat.com/2012/09/04/estonia-code-academy/, zuletzt geprüft am 05.05.2014.

Kempf, Dieter (2012): Pressekonferenz von BITKOM und BKA Cyberkriminalität und IT-Sicherheit. Berlin, 17.09.2012.

Kempf, Dieter; Wallraf, Bruno (2014): Pressekonferenz Cloud Monitor 2014. Berlin, 30.01.2014.

KPMG (2004): Report IT-Umfrage 2004.

Kurki, Lauri Ilari (2006): Informationssicherheit in österreichischen klein- und mittelständischen Unternehmen. Diplomarbeit. Fachhochschule Informationsberufe, Eisenstadt. Informationstechnologie.

Lacey, David (2010): Understanding and transforming organizational security culture. In: *Information Management & Computer Security* 18 (1), S. 4–13.

Lacey, David; James, Barry E. (2010): Review of Availability of Advice on Security for Small/Medium Sized Organisations. Information Commissioner's Office.

Minister of Economic Affairs and Communications (2006): Estonian Information Society Strategy 2013. Tallinn, zuletzt geprüft am 17.10.2013.

Minister of Economic Affairs and Communications (2012): Estonian Information Society Yearbook, zuletzt geprüft am 17.10.2013.

Ministry of Defence Estonia (2008): Cyber Security Strategy. Tallinn, zuletzt geprüft am 17.10.2013.

Ministry of Security and Justice Netherlands (2011): National Cyber Security Strategy (NCSS). Strength through cooperation.

Ministry of Security and Justice Netherlands (2013): National Cyber Security Strategy 2. From awareness to capability.

National Cyber Security Alliance; Symantec (2012): 2012 National Small Business Study.

National Cyber Security Centre (NCSC) (2012): 2nd Cyber Security Assessment Netherlands (CSBN-2).

National Cyber Security Centre (NCSC) (2013): 3rd Cyber Security Assessment Netherlands (CSAN-3).

National Post and Telecom Agency (PTS) (2005): Swedish strategy to secure the Internet infrastructure. Stockholm.

National Post and Telecom Agency (PTS) (2006): Strategy to improve Internet security in Sweden. Stockholm.

Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) (2011): Factsheet SENTINELS. A research program on security in ICT, networks and information systems. Online verfügbar unter http://www.sentinels.nl/sites/stw.demo.infi.nl/files/mediabank/2011%20SENTINELS%20Factsheet.pdf.

Nowey, Thomas; Federrath, Hannes; Riesner, Moritz (2009): Expertenstudie zum Sicherheitsmanagement in deutschen Organisationen. Institut für Wirtschaftsinformatik Universität Regensburg. Regensburg.

OECD (2012): Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (OECD Digital Economy Papers, 211).

Office for National Statistics UK (ONS UK) (2013a): E-Commerce and ICT Activity, 2012. Statistical Bulletin. Online verfügbar unter http://www.ons.gov.uk/ons/rel/rdit2/ict-activity-of-uk-businesses/2012/stb-ecom-2012.html.

Office for National Statistics UK (ONS UK) (2013b): Social Networking: The UK as a Leader in Europe. Online verfügbar unter http://www.ons.gov.uk/ons/rel/rdit2/internet-access---households-and-individuals/social-networking--the-uk-as-a-leader-in-europe/sty-social-networking-2012.html, zuletzt geprüft am 21.05.2014.

Park, Ji-Yeu; Robles, Rosslin J.; Hong, Chang-Hwa; Yeo, Sang-Soo; Kim, Tai-hoon (2008): IT Security Strategies for SME's. In: *International Journal of Software Engineering and Its Applications* 2 (3), S. 91–98.

Ponemon Institute (2012): State of SMB Cyber Security Readiness: UK Study. Traverse City.

Ponemon Institute (2013): 2013 Cost of Data Breach Study: Global Analysis. Traverse City.

Reisinger, Philipp (2013): Informationssicherheit in Österreich. Eine Studie zur Informationssicherheit in österreichischen Unternehmen. Bachelorarbeit. Fachhochschule St. Pöllen, St. Pöllen.

Sánchez, Luís E.; Santos-Olmo Parra, Antonio; Rosado, David G.; Piattini, Mario (2009): Managing Security and its Maturity in Small and Medium-sized Enterprises. In: *Journal of Universal Computer Science* 15 (15), S. 3038–3058.

Schubert, Susanne; Rhiel, Mathias (2013): Der IT-Sicherheitsmarkt in Deutschland. Grundstein für eine makroökonomische Erfassung der Branche. Bundesministerium für Wirtschaft und Technologie (BMWi). Berlin.

Swedish Civil Contingencies Agency (MSB) (2011): Strategy for information security in Sweden. Karlstad.

Symantec (2010): Symantec Survey Reveals Information Protection is the Highest IT Priority for SMBs. Average SMB now spends approximately $51,000 a year to protect their information. Online verfügbar unter http://www.symantec.com/about/news/release/article.jsp?prid=20100621_01.

Teuteberg, Frank (2010): IT-Risikomanagement – Eine Studie zum Status quo in deutschen Unternehmen. In: Frank Keuper und Fritz Neumann (Hg.): Corporate Governance, Risk Management und Compliance. Innovative Konzepte und Strategien. Wiesbaden: Gabler, S. 69–89.

TU Wien (18.02.2013): Sicherheitsrisiko Mensch? Wie sicher sind unsere Daten im Internet? Online verfügbar unter http://www.tuwien.ac.at/aktuelles/news_detail/article/8026/.

Verband der Versicherungsunternehmen Österreichs (VVO) (24.04.2014): Internetkriminalität in Österreich - die unterschätzte Gefahr! Wien. Online verfügbar unter http://www.vvo.at/cybercrime-aktualisieren-sie-ihre-kontodaten.html, zuletzt geprüft am 06.05.2014.

Wirtschaftskammer Österreich (WKÖ) (2014a): IT Sicherheitshandbuch für KMU. Datensicherheit schafft Vorsprung. 6. Aufl. Online verfügbar unter https://www.wko.at/Content.Node/it-safe/kmu_handbuch_komplett.pdf, zuletzt geprüft am 06.05.2014.

Wirtschaftskammer Österreich (WKÖ) (2014b): IT Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter. 5. Aufl. Online verfügbar unter https://www.wko.at/Content.Node/it-safe/mitarbeiter_handbuch_komplett.pdf, zuletzt geprüft am 06.05.2014.